UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

AMERICAN CIVIL LIBERTIES UNION, et al., Plaintiffs, v. ALBERTO R. GONZALES, in his official capacity as ATTORNEY GENERAL OF THE UNITED STATES, Defendant.	Civ. Act. No. 98-CV-5591

PRE-TRIAL ORDER

I. Jurisdiction

Plaintiffs' complaint arises under the United States Constitution and the laws of the United States and presents a federal question within this Court's jurisdiction under Article III of the federal Constitution and 28 U.S.C. §§ 1331 and 1361. Defendant has challenged Plaintiffs' standing and, therefore, whether there is Article III jurisdiction over their claims.

II. Facts

A. Stipulated Facts

1. Defendant, Alberto R. Gonzales, is the Attorney General of the United States, who is charged with enforcing the provisions of the Child Online Protection Act ("COPA") challenged in this action.

2. Plaintiffs represent a range of individuals and entities including speakers, content providers, and ordinary users on the World Wide Web (the "Web"), as that term is defined in the Act. Plaintiffs post content including, *inter alia*, resources on sexual health, safe sex, and sexual education; visual art and poetry; resources for gays and lesbians; online magazines and articles; music; and books and information about books that are being offered for sale.

3. Some of the Plaintiffs provide interactive fora on their Web sites, such as online discussion groups, bulletin boards and chat rooms, which enable users to create their own material on Plaintiffs' Web sites. Some of the verbal and visual exchanges that could potentially occur in these chatrooms or in the postings on their bulletin boards may include language or images that contain sexual content.

4. Plaintiff ACLU is a nationwide, non-partisan organization which states that it is dedicated to defending the principles of the Bill of Rights. ACLU members Patricia Nell Warren and Lawrence Ferlinghetti engage in speech on the Internet.

5. Plaintiff ACLU sues in part on behalf of its member Lawrence Ferlinghetti, who is a writer and San Francisco's poet laureate. Mr. Ferlinghetti is the co-founder of City Lights Bookstore, which maintains a website "that promotes books available from the bookstore" and "contains lists of literary events and a brief history of City Lights Bookstore and Publishing," has a section describing Mr. Ferlinghetti's 1956 obscenity trial for selling the Allen Ginsberg poem "Howl," and also has Mr. Ferlinghetti's poetry.

6. The City Lights Bookstore website states that "City Lights is a landmark independent bookstore and publisher that specializes in world literature, the arts, and progressive politics." The website also states that:

> For almost half a century, City Lights has demonstrated a commitment to preserving and promoting the diversity of voices and ideas that are represented in

> quality books. Now, as information technologies change the way people live and think, we are convinced that a community that continues to value writing and reading is essential to the future of a democratic society. With this in mind, we formed the City Lights Foundation, a non-profit cultural and educational foundation with the goal of advancing literacy and the literary arts.

7. Plaintiff ACLU also sues in part on behalf of Patricia Nell Warren, who is an author of novels, poetry, numerous articles, and essays. Her novels are alleged to be the most popular novels among classic gay literature. Ms. Warren is a co-owner of Wildcat International and its publishing arm, Wildcat Press. The website for Wildcat Press contains excerpts of her work, including "sexually explicit details such as the description of a 'foursome' erotically dancing and a description of two men passionately kissing." The Wildcat International website states that "Wildcat International is an independent media company offering the real edge in writing, publishing, filmmaking, special events, and media consulting."

8. Plaintiff Condomania states that it is the nation's first condom store and a leading seller of condoms and distributor of safer sex materials. Condomania engages in speech on the Internet.

9. Plaintiff Heather Corinna Rearick is a writer, artist, sex-educator, and activist whose primary presence on the Web consists of Scarletletters.com, Scarleteen.com, and Femmerotic.com.

10. Plaintiff Heather Corinna Rearick alleges that she maintains three websites, "each of which deals with issues of sex and sexuality with an explicit focus on challenging and combating the sexual oppression of traditionally marginalized groups."

11. Ms. Rearick operates the website scarleteen.com. "Scarleteen is the Internet's largest independent, unaffiliated, free resource for young adult sex education, information, and discussion, serving nearly two million teens, young adults, parents, and educators each year."

The Scarleteen website states that "[w]e offer Scarleteen as a far better resource for sex information for teens than adult sexuality sites, as well as a supplement to in-home and school-based sex education. Many parents we have heard from have used it as a tool to initiate discussion with their teens on some of the topics addressed. Homeschooling parents have used Scarleteen as curricula for sex education; colleges add our articles to their syllabi often."

12. "Femmerotic is Heather Corinna [Rearick]'s personal Web site for showcasing her photographic and textual work and providing an 'open and intimate look at her life as an artist and activist.'" On this website Ms. Rearick states that "[g]enerally, I intend to examine sexuality, to document sexual relationship, to explore the human body and how I and viewers perceive it, to examine the female body and feelings about it, to explore my own identity and use all those aims to create work that creates questions."

13. Plaintiff Electronic Frontier Foundation ("EFF") sues in part on behalf of John W. "Bill" Boushka, who has work on the website www.doaskdotell.com. In the Amended Complaint, Mr. Boushka states that he fears prosecution for his book "Do Ask, Do Tell: A Gay Conservative Lashes Back," which he describes as "an exposé about gays in the military" that is a "politically-charged text" containing "subject-matter and language that might be deemed harmful to minors." Doaskdotell.com states that "[t]his site (with the sister site[] . . . billboushka.com) presents an objective approach (that I call 'Do Ask, Do Tell') to social and political issues ("sociology"), where arguments and counter-arguments are directly compared."

14. Another website Mr. Boushka mentions in the Amended Complaint, hppub.com, is now defunct.

15. Plaintiff Free Speech Media, in partnership with Public Communicators Inc., operates freespeech.org, which provides speech on the Internet.

16. Plaintiff Free Speech Media, LLC operates a website "designed to encourage the democratic expression of progressive ideals through promoting, curating and hosting independent creators of audio and video content on the Web." Its video and audio files "cover a wide range of topics, including human rights, homelessness, labor issues, racism, prison conditions, sexuality, AIDS, feminism and environmentalism." The Free Speech TV website states that "[s]eizing the power of television to expand social consciousness, FSTV fuels the movement for progressive social, economic, and political transformation. By exposing the public to perspectives excluded from the corporate-owned media, FSTV empowers citizens to fight injustices, to revitalize democracy, and to build a more compassionate world." The websites also states that "Free Speech TV broadcasts independently-produced documentaries dealing with social, political, cultural, and environmental issues; commissions and produces original programming; develops programming partnerships and collaborations with social justice organizations; provides special live broadcasts from remote locations; and maintains an adjunct Web site that hosts one of the Internet's largest collection of progressive audio and video content."

17. Plaintiff Nerve.com, Inc. is an online magazine which states that it is devoted to sexual literature, art, and politics. Nerve.com is run by Rufus Griscom.

18. Plaintiff Aaron Peckham d/b/a Urban Dictionary operates an online dictionary of contemporary slang.

19. Plaintiff Aaron Peckham d/b/a Urban Dictionary operates "an online slang dictionary whose terms and definitions are solely user-generated and user-rated."

20. Plaintiff Philadelphia Gay News states that it has been the leading print newspaper for the gay and lesbian community in Philadelphia since 1976. It is now published on the Internet.

21. Plaintiff Philadelphia Gay News ("PGN") is the "oldest gay newspaper in Philadelphia" and publishes both in print and online. The online and print editions "share much of the same content, including national and local news stories written by PGN correspondents, arts and events sections, regular columns, a calendar of events, and editorials on a variety of social and political topics." The online edition also contains personal and classified advertisements.

22. Plaintiff American Booksellers Foundation For Free Expression (ABFFE) is a non-profit organization founded by the American Booksellers Association. Plaintiff Powell's Bookstore is a member of ABFFE.

23. Plaintiff Powell's Bookstore operates seven bookstores in Portland, Oregon. Powell's has a web site.

24. Plaintiff Powell's Bookstores states that it is the "world's largest independent new and used bookstore" and operates a website that "allows users to browse and purchase new, used, rare, and out-of-print books."

25. Plaintiff Salon Media Group publishes an online magazine featuring articles on current events, the arts, politics, the media, and relationships.

26. Plaintiff Salon Media Group, Inc. ("Salon") states that it "is a well-known, popular on-line magazine" that contains "news articles; commentaries on and reviews of music, art, television, and film; and regular columns on politics, relationships, the media, business, and other areas of interest." Salon's "goal is to break news as well as produce the most compelling

sort of social commentary . . . on the web," and it seeks to attract a "broad general interest audience" with its readership.

27. Plaintiff Sexual Health Network owns and operates sexualhealth.com, which is dedicated to providing easy access to sexuality information, education, and other sexuality resources. Sexual Health Network is owned and operated by Mitchell Tepper.

28. Plaintiff Sexual Health Network has a website "dedicated to providing easy access to sexuality information, education, support and other sexuality resources for everyone, including those with disability, chronic illness or other health-related problems." It is run by Dr. Mitchell Tepper, who has a doctorate in Human Sexuality Education and a master's degree in Public Health. The Sexual Health Network website provides information to minors, as well as adults.

29. Plaintiff Electronic Privacy Information Center ("EPIC") "is a nonprofit educational organization established in 1994 to examine civil liberties and privacy issues arising on the Internet." EPIC alleges that it accesses information on the Internet, including sexually explicit pages, as part of its mission, which includes reporting on how well content filters work.

30. All of the plaintiffs express a subjective fear of prosecution under the statute.

31. No Plaintiff has ever been contacted by state or local authorities, nor prosecuted nor arrested regarding any investigation into criminal violations.

32. Every Plaintiff has Web pages that are blocked by at least two filtering companies in categories designed to assist parents in protecting their children from inappropriate speech about sex.

33. Ms. Warren acknowledges the serious literary value of her works, as the Wildcat International website states: "Patricia Nell Warren's novels have become essential gay literature

for bookstores, libraries and college courses worldwide and, according to recent surveys of independent book sales, are the most popular novels among classic gay literature." Ms. Warren believes that adults and minors "should have the right to access speech provided on the Wildcat Web site."

34. The Scarleteen.com web pages identified by Plaintiff Rearick as representative of those about which she fears prosecution include website's front page, the discussion group front page, and the "front pages, and 'Articles' and 'Advice' subsections" of the website sections entitled: Body, SexYOUality, Reproduction, Infection Section, Pink Slip, Boyfriend, Take Two, Gaydar, and Sexual Politics.

35. Scarlet Letters is a website containing works of an artistic nature. The website states, "Since February of 1998, Scarlet Letters has been one of the web's premier publisher of humanist, feminist, sex positive original and visionary creative and artistic work of all kinds." Furthermore, the website states, "Our goal is to give our readers an international and unique perspective on artistic expression without pretension or arbitrary limits."

36. Ms. Rearick describes her work on the photography home page in this manner:

> Blending more traditional styles, archetypes and themes with new approaches, keeping the physical and emotional tone real, grounded, varied and intense, I try to step outside genre by creating work that explores sexuality, gender and personal identity within fine art without a typical fine art nude genericism or loss of personal identity of the subject.

37. Free Speech Media identified five videos as a representative sample upon which it fears prosecution. Free Speech also stated that it maintains a community page, which contains material and links that "contain or may contain in the future, among other things, candid and explicit comments or questions on a diverse category of topics posted directly by internet web

users." Some of the videos identified by Free Speech Media in its Amended Complaint and in discovery are no longer available on the website.

38. Nerve has won multiple awards for both its prose and photography." Nerve was one of five finalists for the National Magazine Award for General Excellence Online in 2005, along with Atlantic Monthly, Consumer Reports, Business Weekly and Style.com.

39. Nerve states in a general manner that its website "includes many photographs of nude and semi-nude persons taken by professional photographers such as Nan Goldin, Bettina Rheims, and Sylvia Placy, and by the site's own users."

40. In response to interrogatories, Nerve listed material in four sections about which it fears prosecution: the website's nominations for its "Henry Miller Award" in the fiction section; the free tour available within the photography section, the "Blog-A-Log" section, in which readers can read about the dating experience of Nerve contributors in personal blogs, and the blog section of the website.

41. Mr. Peckham's asserted fear of prosecution is based on the fact that "Urban Dictionary contains material that may be considered 'harmful to minors' in some communities," because "[d]ozens of the words, phrases, and definitions found on urbandictionary.com humorously, graphically, or symbolically describe human anatomy and sexual acts." In the Amended Complaint and in response to Interrogatories, Mr. Peckham listed slang terms for which he feared prosecution.

42. Urban Dictionary is designed for users to share definitions of a variety of slang words, including words of a sexual nature. Mr. Peckham asserts that "Letters to the site from students, parents, lawyers, educators, reporters, media translators and lexicographers attest to the site's cultural significance."

43. Philadelphia Gay News ("PGN") fears prosecution because it deals with "issues relevant to the gay and lesbian community," that "some communities would consider access to personal advertisements inappropriate for minors when involving persons of the same gender," and that "some communities" may believe PGN's descriptions of social and sports clubs catering to the gay and lesbian community to be harmful to minors "because they 'entice' young people into exploring gay life."

44. PGN identified printouts of web pages about which it fears prosecution. Many of the pages about which PGN alleged a fear of prosecution, such as the "Philly Encounters" section and advertisements therein, as well as chat rooms, are no longer on the website.

45. ABFFE explained the type of material that its members seek to access. ABFFE describes it as material that contains "nudity and sexual conduct," such as the books *Primary Colors* by Anonymous and *Sabbath's Theater* by Philip Roth.

46. EPIC fears that if COPA were to go into effect the websites it reviews "may remove from their Web sites material similar to that which EPIC staff heretofore have been able to access" without providing proof of age. EPIC alleges that COPA compromises the right to access speech anonymously and that it "does not intend to instruct its staff to use a credit card or adult access code" to access websites.

47. Philip Stark is a Professor of Statistics at the University of California, Berkeley. He has been on the Statistics faculty at that university since 1988.

48. Philip Stark has been a Miller Research Professor, a Dodson Fellow, a Presidential Chair Fellow, and a Mellon/Library Faculty Fellow.

49. Philip Stark received a Bachelor's degree from Princeton University in 1980 and a Ph.D. from the University of California, San Diego, in 1986.

50. Philip Stark was a Presidential Young Investigator and a National Science Foundation Postdoctoral Fellow in Mathematical Sciences.

51. Philip Stark has been on the editorial board of several journals, and has written over 65 articles and technical reports.

52. Philip Stark has given approximately 130 invited lectures at scientific conference and universities in 16 countries.

53. Philip Stark has testified before the U.S. House of Representatives' Subcommittee on the Census and the California Senate's Natural Resources Committee.

54. Philip Stark has consulted for the U.S. Department of Justice, the Federal Trade Commission, the U.S. Department of Agriculture, the U.S. Census Bureau, the U.S. Attorney's Office for the Northern District of California, the U.S. Department of Veterans Affairs, the Los Angeles County Superior Court, the National Solar Observatory, public utilities, major corporations, and numerous law firms.

55. Philip Stark has testified as an expert witness, or has served as a non-testifying expert, in cases involving antitrust, consumer class actions, employment discrimination, equal protection, fairness in lending, federal legislation, insurance, intellectual property, product liability, trade secrets, truth in advertising, and wage and hour disputes.

56. Some of Philip Stark's consulting and research relates to the Internet, including characterizing and predicting online consumer behavior and developing search algorithms.

57. Philip Stark created a web-based statistics course using HTML, JavaScript and Java, the most widely used web languages.

58. Philip Stark has been on the advisory boards of a web marketing firm and two online publishers.

59. Paul Mewett is a Principal in the London office of CRA International. He is the head of the Internet Intelligence Unit, which supports both CRA's Forensic Investigations Practice and it Computer Forensics Practice.

60. Over the last ten years, all of Paul Mewett's major projects have involved the Internet. For the past 25 years, his specialty has been in assisting organizations to evaluate and implement new technologies.

61. Paul Mewett served as an electronics engineer for the British Ministry of Defense, and received electronics qualifications from the School of Royal Electrical and Mechanical Engineers for the Ministry of Defense in 1984.

62. Dr. Eisenach is an expert on the Internet and its impact on markets and public policy.

63. Dr. Eisenach has performed studies on the use of Microsoft's Internet Explorer and Operating Systems software, as well as of the use of peer-to-peer software.

64. Dr. Eisenach is the Chairman of Criterion Economics, LLC, an economic and financial consulting firm based in Washington, D.C. Prior to joining Criterion Economics, LLC in 2006, Dr. Eisenach was Chairman of CapAnalysis, LLC, an economic and financial consulting firm based in Washington, D.C.

65. Dr. Eisenach received a Ph.D. in economics from the University of Virginia in May 1985, and has taught economics and/or public policy at the Kennedy School of Government at Harvard University, George Mason University Law School, the University of Virginia, and Virginia Polytechnic Institute and State University.

66. Dr. Eisenach has co-edited scholarly books on antitrust issues in the market for computer operating systems and applications, and on the role of government regulation of telecommunications markets.

67. Since 1999, Dr. Stephen Neale has been a Professor of Philosophy at Rutgers University, where he holds the rank of Professor II, a special designation within the rank of (Full) Professor.

68. Dr. Neale is an affiliated member of the Department of Linguistics at Rutgers and the Center for Cognitive Science.

69. Dr. Neale has been a Guggenheim fellow, a Rockefeller fellow, a fellow of the National Endowment for the Humanities (NEH), and a President's Fellow of the University of California.

70. Dr. Neale has published widely in peer review journals and other refereed academic publications, and he has lectured around the world over the past twenty years, as an invited speaker at both academic institutions and professional conferences in philosophy, linguistics, mathematical logic, and computer science.

71. Dr. Neale was a professor at the University of California, Berkeley from 1990 to 1998, where he was tenured in 1993 and promoted to Full Professor in 1998. At Berkeley, he was a member of the Graduate Program in Logic and Methodology of Science, which he chaired for several years.

72. Dr. Neale was an Assistant Professor of Philosophy and Linguistics at Princeton University from 1988 to 1990 and a member of the Program in Cognitive Science.

73. Dr. Neale received his Ph.D. from Stanford University in 1988. He began his doctoral work in the Ph.D. program in linguistics in the Department of Linguistics and

Philosophy at MIT in 1983, moved to the PhD program in linguistics at Stanford in 1984, and obtained the PhD in the field of philosophy in 1988 with a dissertation bridging linguistic semantics and the philosophy of language.

74. Defendant's expert witness, Arthur E. Clark, Jr., has thirty-five years of industry experience that includes both management positions at American Express, Citigroup, Dow Jones, and management consulting. Mr. Clark has experience in the use of payment cards on the Internet developed from doing consulting projects for Amazon, NetCharge, and American Express. Mr. Clark also has experience with assisting banks in developing prepaid cards for the youth market. In addition, Mr. Clark has experience with assisting acquiring banks in signing up new merchants and with assisting banks in developing secured payment cards for unbanked persons. Mr. Clark has served as expert witness relating to payment cards in four other cases.

75. Mr. Clark graduated Colgate University with a B.A. in Economics in 1969. Mr. Clark graduated from New York University Graduate School of Business with a M.B.A. with a major in Marketing in 1971.

76. Scott M. Smith, Ph.D., is the James M. Passey Professor of Marketing and Director of the Institute for Marketing in the Marriot School of Management, Brigham Young University.

77. Dr. Smith is the co-author of the textbook *Fundamentals of Marketing Research* (Sage Publications, 2005) and the PC-MDS statistical software programs for multidimensional statistical analysis. He authored or co-authored 12 books and monographs and more than 60 articles and papers. He has published in *Marketing Research, Journal of Marketing Research, Journal of Consumer Research, Journal of Business Research, Journal of the Academy of Marketing Science, Journal of Marketing Education* (awarded the year's outstanding article), and

Journal of Business Ethics. The academic books also include, *Multidimensional Scaling, Computer Assisted Decisions in Marketing,* and *Internet Marketing*.

78. The Internet is an interactive medium based on a decentralized network of computers.

79. On the World Wide Web, a client program called a Web browser retrieves information resources, such as Web pages and other computer files, from Web servers using their network addresses and displays them, typically on a computer monitor, using a markup language that determines the details of the display. One can then follow hyperlinks in each page to other resources on the World Wide Web of information whose location is provided by these hyperlinks. The act of following hyperlinks is frequently called "browsing" or "surfing" the Web.

80. Web pages are often arranged in collections of related material called "Web sites," which consist of one or more "Web pages."

81. To navigate to different pages on the Web, an HTTP request is sent to the Web server working at that IP address for the page required. In the case of a typical Web page, the HTML text, graphics and any other files that form a part of the page will be requested and returned to the client (the Web browser) in quick succession. The Web browser's job is then to render the page as described by the HTML and other files received, incorporating the images, links and other resources as necessary. This produces the on-screen "page" that the viewer sees. Most Web pages contain hyperlinks to other relevant and informative pages and perhaps to downloads, source documents, definitions and other Web resources.

82. Some Web sites serve as a proxy or intermediary between a user and another Web page. When using a proxy server, a user does not access the page from its original URL, but rather from a URL on the proxy server.

83. Modern search engines search for and index web pages individually. Search engines are web sites that provide links to relevant web pages, in response to search terms (words or phrases) entered by a user. They are a popular way of finding information online.

84. Most users interact with the Web by using a search engine. A search engine is a computer program designed to help find information stored on a computer system such as the World Wide Web. The search engine allows the user to request content that meets specific criteria (typically those containing a given word or phrase) and to retrieve a list of references that match those criteria.

85. Internet content filtering software attempts to block certain categories of material that a Web browser is capable of displaying, including "adult" material. Filters categorize Web sites or pages based on their content. By classifying a site or page, and refusing to display it on the user's computer screen, filters can be used to prevent children from seeing material that might be considered unsuitable. In addition, businesses often use filters to prevent employees from accessing Internet resources that are either not work related or otherwise deemed inappropriate.

86. Some Internet content filters can be purchased on a CD or downloaded from the Internet and installed on a personal computer. Some filters are designed to be run on a server in a corporate, library, or school environment. Other filters are built into the services provided by Internet Service Providers.

87. Filters use different mechanisms to attempt to block access to material on the Internet. Some filters use "black lists" to filter out content. Black lists are lists of Web site addresses (URLs) or Internet Protocol (IP) addresses that a filtering company has determined point to content that contains the type of materials their filter is designed to block.

88. In list-based filtering (sometimes called database or static filtering), the software draws on a database of pre-classified URLs and/or IP addresses. When a user requests a Web page (by entering a URL or IP address into a Web browser, or by clicking on a link) the filtering software checks it against the database and responds in whichever way it has been configured to respond.

89. A filter that allows access only to Web sites that have been thoroughly checked and found to contain no content in a certain category is called a "white list."

90. Some filters also use "white lists" of content that should never be blocked. White lists are lists of URLs or IP addresses that the filtering company has determined do not point to any content their filter is designed to block. A very restrictive filter might block all URLs except those included on a white list.

91. In addition to their own black and white lists, some filtering products give parents or administrators the option of creating customized black or white lists.

92. In addition to relying on black lists and white lists, some filters also use "key words" or other "dynamic filtering" techniques to attempt to limit access to certain Web pages. Filtering companies may compile lists of words and phrases associated with content that should be blocked, even if the page has not previously been categorized. Some products just attempt to remove those words from the page, while others attempt to block the entire Web page that contains these words or phrases.

93. A filter that responds solely to the text making up the name of an image file (*e.g.*, blowjob03.jpg) is a text-based filter, not an image-based filter. Similarly, filters that respond solely to the text making up the names of audio files (*e.g.*, screamingorgasm.mp3) or video files (*e.g.*, blowjobs.jpeg) are text-based filters (not audio-based or video-based filters).

94. Browsing the World Wide Web is one way in which individuals can use the Internet. The Internet can be used to engage in activities such as sending and receiving emails, trading files, exchanging instant messages, chatting online, streaming audio and video, and making voice calls.

95. Some filtering programs can be used by parents to prevent their children from having any access to parts of the Internet other than the Web, and to certain Internet applications which parents do not want their children to have any access to, such as e-mail, chat, instant messaging, newsgroups, message boards, and peer-to-peer file sharing.

96. Some content from the Internet is now capable of being viewed on devices other than traditional personal computers. Examples include mobile devices such as mobile phones, personal digital assistants ("PDAs") such as the Blackberry, portable audio/video players such as the iPod, and game consoles such as the XBox or PlayStation.

97. The U.S. Census Bureau's Current Population Survey's results show that in September 2001, approximately 54 percent of the U.S. population was using the Internet from any location. That figure rose to 59 percent in 2003.

98. According to Marv Johnson, legislative council for the ACLU, the creation of a "dot-xxx" top-level domain name is "not going to make a whole lot of difference" in stopping minors from finding pornography. (http://www.physorg.com/news12015.html)

99. Parents of minor children who borrow their parent's payment cards to make online purchases can ask their children what they are going to purchase.

100. The City Lights Bookstore website accepts payment cards on order pages for customers and on a donation page to the City Lights Bookstore foundation.

101. The Wildcat International website accepts payment cards on order pages for customers, retailers, and educational booksellers.

102. The Condomania website accepts payment cards on order pages for customers.

103. The Scarleteen website links users to PayPal, which accepts payment cards, for donations to help Scarleteen continue to provide comprehensive sex education. The Scarleteen website shop links users to second-party sellers that accept payment cards on order pages for users.

104. The Scarlet Letters website has a membership subscription page that links users with a second-party site that accepts payment cards. Membership is required for "access to all Scarlet's past issues and membership to Heather Corinna to boot, with nearly 4,000 original, high quality erotic photographs, fiction, poetry and nonfiction from the editor and founder of Scarlet Letters."

105. The Femmerotic website has a membership subscription page which takes users to a second-party site that accepts payment cards. Among other things, members obtain access to "[o]ver 5,000 of [Ms. Rearick's] high-quality, mindfully and independently produced fine art photographs . . . . Erotic and nonerotic portraiture, fine art nudes, gender and body image exploration, installation projects, drag, couples photography, and primarily intimate, personal self-portraiture."

106. The Free Speech Media website accepts payment cards at its online merchandise store. The Free Speech Media website also accepts payment cards for donations to help Free Speech Media.

107. The Urban Dictionary website's book section links users to Amazon.com, which accepts payment cards.

108. Salon restricts access to large portions of its website to viewers that either watch a video advertisement in order to get access for the day or to viewers that are subscribers. The Salon website has a membership subscription page that accepts payment cards. A Salon membership "support[s] independent journalism" and allows the user access to all Salon articles and the discussion forum. The online store on the Salon website links users to second-party sellers that accept payment cards.

109. The online store on the Sexual Health Network website links users to second-party sellers that accept payment cards.

110. FTP stands for file transfer protocol. It is used primarily to transfer files across the Internet.

111. HTTP stands for hypertext transfer protocol; it is widely used on the Internet.

112. Among the web sites that use primarily HTTP are *The New York Times, Washington Post,* and even plaintiffs ACLU, Electronic Frontier Foundation, Electronic Privacy Information Center, and Salon Media Group.

113. Most URLs use HTTP.

114. The FBI, which is part of the Department of Justice, uses the Websense enterprise filter for its computers with access to the Internet. The FBI installed Websense to block content, such as advertisements on the Internet taking up large bandwith, and to protect the institution

from malicious codes and waste, fraud, and abuse of the Internet. Among the content blocked is content falling in the categories of pornographic and illicit adult material. Overall, the FBI is satisfied with the effectiveness of Websense to block content, although there have been reports of overblocking. The FBI has not performed an audit on the effectiveness of the Websense enterprise product in blocking sexual material.

115. The Bureau of Alcohol, Tobacco and Firearms, which is now part of the Department of Justice, uses the SmartFilter enterprise filter for its computers with access to the Internet. The ATF installed SmartFilter to block content, including sexually explicit material. The ATF reports that the SmartFilter product has fulfilled the requirements of the its business needs, although there have been reports of overblocking. The ATF has not performed an audit on the effectiveness of the SmartFilter enterprise product in blocking sexual material.

116. The Federal Bureau of Prisons (BOP), which is part of the Department of Justice, uses the SurfControl enterprise filter for its computers with access to the Internet. The BOP installed SurfControl to assist it in enforcing its policy that access to the Internet on BOP computers by its employees be primarily for the purpose of performance of official duties and to protect from waste, fraud, and abuse of the Internet. In furtherance of these objectives, BOP utilizes many of the categories provided by SurfControl, including the category that seeks to block sexually explicit web content. If a BOP employee requests that a website be unblocked by SurfControl, he or she must obtain approval of his or her supervisor and the sole reason for consideration of unblocking any website is that access to the website is required solely for performance of official duties. BOP has a policy of denying such requests for personal reasons. Overall, the BOP is satisfied with the effectiveness of Surfcontrol to block content, although there have been reports of overblocking.

117. It is an affirmative defense to prosecution under COPA to restrict, in good faith, access by minors to material that is harmful to minors by requiring use of a credit card.

118. It is an affirmative defense to prosecution under COPA to restrict, in good faith, access by minors to material that is harmful to minors by requiring use of a debit card, including a reloadable prepaid card.

119. COPA does not reach non-commercial speech, even on the World Wide Web. 47 U.S.C. §231(a)(1); (e)(2)(A).

120. Congress has required Internet service providers (ISPs) and online service providers to "notify [all new customers] that parental control protections (such as computer hardware, software or filtering services) are commercially available that may assist the customer in limiting access to material that is harmful to minors." 47 U.S.C. § 230(d). Congress also passed legislation that mandates the use of filtering programs in public schools and libraries that receive funds under two popular federal programs.

B. Plaintiffs' Statement of Facts that Are in Dispute

I. PLAINTIFFS

1. Many of the Plaintiffs are committed to providing uncensored Web sites.

2. The vast majority of information on Plaintiffs' Web sites, as on the Web in general, is provided to users for free.

3. Similarly, the vast majority of information on Plaintiffs' Web sites, as on the Web in general, can be accessed immediately without any requirement that users register, provide a password or log-in, or otherwise provide any personal, identifying information in order to access the material.

4. Plaintiffs are commercial speakers on the Web. The speech on Plaintiffs' Web sites is designed to assist in making a profit. Although many of the Plaintiffs believe that much of the information available on their Web sites has non-commercial value, all of the information meets the definition of "for commercial purposes" under the Act.

5. Plaintiffs, like the universe of commercial speakers on the Web, have a variety of business models. Some of the Plaintiffs receive income by selling advertising on their Web sites. Some of the Plaintiffs sell goods over their Web sites, ranging from millions of books, to condoms and other sexual health devices, to books that they authored themselves. Some of the Plaintiffs use the Web simply as an advertising and marketing tool -- a means of promoting their commercial activities. Some of the Plaintiffs generate revenue by combining these or utilizing other business models.

6. Web sites, including Plaintiffs' Web sites, depend on attracting a high level of traffic to their sites to attract and retain advertisers and investors.

7. The best way to stimulate user traffic on a Web site is to offer some content for free to users.

8. With respect to those Plaintiffs and others who sell goods on their Web sites, only a small percentage of Internet users who visit those Plaintiffs' sites for information actually make a purchase.

9. Although all of Plaintiffs' speech is commercial within the meaning of the statute, Plaintiffs believe that all of their speech has value, especially for adults and older minors.

10. If the Act is not permanently enjoined, some of the Plaintiffs intend to self-censor; others intend to risk liability and prosecution under the Act; and others have not yet decided what they will do. At least one Plaintiff has decided that, because it would be contrary to its mission to

self-censor, it will have to forego the financial benefits of its commercial activities and become a noncommercial site if the Act is not permanently enjoined.

11. Plaintiff EFF is a nationwide nonprofit organization that is committed to defending civil liberties in the world of online computer communication. EFF members access speech on the Internet.

12. Plaintiff EPIC is a non-profit research organization that collects and distributes information concerning civil liberties and privacy issues arising in the new communications media. EPIC contributors access speech on the Internet.

II. PLAINTIFFS AND OTHER SPEAKERS REASONABLY FEAR PROSECUTION AS A RESULT OF COPA.

13. Defendant's definition of speech covered by COPA has been inconsistent and unclear.

14. Speech similar to that of Plaintiffs has been the subject of extensive efforts at censorship and prosecution around the country in recent years. In most cases, those efforts have been based on the importance of protecting children from speech about sex that adults consider harmful, patently offensive, and without value.

15. There are numerous examples of material on Plaintiffs' Web sites that contains nudity, sexual imagery, depictions or descriptions of sexual conduct or sexual acts, frank discussion of sexual topics, or explicit adult language or other matter that might be considered harmful to minors.

16. Members of the ACLU have Web sites that contain speech that describes and depicts sexual acts and sexual contact that is frank and explicit. Although those members believes their speech has value, even for older minors, they reasonably believe that many others do not share that view.

17. Members of ABFFE have Web sites that contain speech that describes and depicts sexual acts and sexual contact that is frank and explicit. Although those members believes their speech has value, even for older minors, they reasonably believe that many others do not share that view.

18. Condomania contains speech that depicts and describes human genitalia, sexual acts, and sexual contact that is frank and explicit. Although Condomania believes its speech has value, even for older minors, Condomania reasonably believes that many others do not share that view.

19. Adam Glickman is aware of other web sites that contain similar speech about human genitalia, sexual contact and sexual activity that are frank and explicit.

20. Members of EFF have Web sites that contain speech that describes and depicts sexual acts and sexual contact that is frank and explicit. Although those members believes their speech has value, even for older minors, they reasonably believe that many others do not share that view.

21. Contributors of EPIC distribute material over the Web that contains speech that describes and depicts sexual acts and sexual contact that is frank and explicit. Although those contributors believes their speech has value, even for older minors, they reasonably believe that many others do not share that view.

22. Free Speech Media contains speech that describes and depicts sexual acts and sexual contact that is frank and explicit. Although it believes its speech has value, even for older minors, Free Speech Media reasonably believes that many others do not share that view.

23. Nerve.com contains speech that depicts and describes sexual acts and sexual contact that is frank and explicit. Although Nerve.com believes that its speech has value, even for older minors, Nerve.com reasonably believes that many others do not share that view.

24. Rufus Griscom is aware of other web sites that contain similar speech about sexual contact and sexual activity that are frank and explicit.

25. Philadelphia Gay News contains speech that describes and depicts sexual acts and sexual contact that is frank and explicit. Although it believes its speech has value, even for older minors, Philadelphia Gay News reasonably believes that many others do not share that view.

26. Powell's Bookstores contains speech that describes and depicts sexual acts and sexual contact that is frank and explicit. Although it believes its speech has value, even for older minors, Powell's Bookstores reasonably believes that many others do not share that view.

27. Sexual Health Network contains speech that describes and depicts sexual acts and sexual contact that is frank and explicit. Although Sexual Health Network believes its speech has value, even for older minors, Sexual Health Network reasonably believes that many others do not share that view.

28. Mitch Tepper is aware of other web sites that contain similar speech about sexual acts and sexual contact that are frank and explicit.

29. Salon.com contains speech that describes sexual acts and sexual contact that is frank and explicit. Although Salon believes its speech has value, even for older minors, Salon reasonably believes that many others do not share that view.

30. Joan Walsh is aware of other web sites that contain similar speech about sexual contact and sexual activity that are frank and explicit.

31. UrbanDictionary.com contains speech that describes sexual acts and sexual contact that is frank and explicit. Although UrbanDictionary.com believes its speech has value, even for older minors, UrbanDictionary.com reasonably believes that many others do not share that view.

32. Aaron Peckham is aware of other web sites that contain similar speech about sexual contact and sexual activity that are frank and explicit.

33. Heather Corrine Rearick operates three web sites that contain speech that depict and describe human genitalia or the post-pubescent female breast, sexual acts, and sexual contact that is frank and explicit. Although Ms. Rearick believes that the speech has value, even, in most instances, for older minors, Ms. Rearick reasonably believes that many others do not share that view.

34. Ms. Rearick is aware of other web sites that contain similar speech about sexual contact and sexual activity that are frank and explicit.

35. Wesley Miller engaged in speech on the outside wall of his art gallery in Pilot Point, Texas that included an image of Eve depicting her post-pubescent female breast. Mr. Miller was threatened with prosecution by the police under a statute prohibiting speech that is harmful to minors.

36. Wayne Snellen is an artist and is Director of the Leslie/Lohman gallery. Mr. Snellen's own art contains speech that depicts human genitalia, sexual acts, and sexual contact, including by same-sex couples, that is frank and explicit. The Gallery contains the work of many other artists whose art is similar and also includes depictions of the post-pubescent female breast. The art is available on the Web. Although Mr. Snellen believes the speech has value, even for older minors, he reasonably believes that many others do not share that view.

37. Mr. Snellen is aware of other web sites that contain similar speech about human genitalia, the post-pubescent female breast, sexual contact and sexual activity that are frank and explicit.

38. Ms. Alicia Smith is a rapper who performs under the name God-Des. Her lyrics contain speech that describes human genitalia, post-pubescent female breasts, sexual acts, and sexual contact that is frank and explicit. Sound clips of her work are available on the Web. Although God-Des believes her speech has value, even for older minors, she reasonably believes that many others do not share that view.

39. God-Des is aware of other web sites that contain similar speech about human genitalia, the post-pubescent female breast, sexual contact and sexual activity that are frank and explicit.

40. Ms. Marilyn Jaye Lewis is the founder and Director of the Erotic Authors Association (EAA), which operates a web site. She is an author herself. Her work and work by other authors can be found on the web site. The web site contains speech that describes human genitalia, the post-pubescent female breast, sexual acts, and sexual contact that is frank and explicit. Although Ms. Lewis believes the speech has value, even for older minors, she reasonably believes that many others do not share that view.

41. Ms. Lewis is aware of other web sites that contain similar speech about human genitalia, the post-pubescent female breast, sexual contact and sexual activity that are frank and explicit.

42. Ms. Barbara DeGenevieve is a visual artist who works in drawings, photographs, articles, and film. Her web site contains speech that depicts and describes human genitalia, the post-pubescent female breast, sexual acts, and sexual contact that is frank and explicit. Although

she believes her speech has value, even for older minors, she reasonably believes that many others do not share that view.

43. Ms. DeGenevieve is aware of other web sites that contain similar speech about human genitalia, the post-pubescent female breast, sexual contact and sexual activity that are frank and explicit.

44. Ninety percent of Internet users have used search engines. When a user does a search, he is given a series of web pages, not web sites, to select. For that and other reasons, it is more accurate to think of a web page "as a whole" than a web site.

45. All of the Web pages categorized by Defendant's expert Paul Mewett as "5(f)" are harmful to minors, as defined by COPA.

46. None of the Web pages categorized by Defendant's expert Paul Mewett as "5(f)" are obscene.

47. All of the Web pages categorized by Defendant's expert Paul Mewett as non-"5(f)" are neither harmful to minors nor obscene.

48. Other than the express words of the statute, Defendant has no policies, guidelines, criteria or rationales for determining whether certain material is "harmful to minors," as defined by COPA.

49. Other than the express words of the statute, Defendant has no policies, guidelines, criteria or rationales for claiming that there is speech that is harmful to minors, but not obscene.

50. Because Defendant has no policies, guidelines, criteria or rationales for determining whether certain material is harmful to minors, a Web site operator has no means of determining whether its Web site is covered by COPA other than by looking at the express words of the statute.

51. According to Defendant, photographs of topless women exposing post-pubescent breasts can be harmful to minors in certain circumstances and not harmful to minors in other circumstances.

52. Defendant has not and cannot identify any criteria or rationale for making the distinction that certain photographs of topless women exposing post-pubescent breasts are harmful to minors in certain circumstances and not harmful to minors in other circumstances.

53. According to Defendant, a photograph of topless women exposing post-pubescent breasts on Playboy.com's Web site is not harmful to minors.

54. According to Defendant, a photograph of topless women exposing post-pubescent breasts on Penthouse.com's website is harmful to minors.

55. According to Defendant, a photograph of a topless woman exposing post-pubescent breasts, where the nipples are covered by superimposed "stars," is harmful to minors.

56. All speech that is prurient for 16 year-olds is prurient for 17 year-olds.

57. All speech that is patently offensive for 16 year-olds is patently offensive for 17 year-olds.

58. All speech that lacks serious literary, artistic, political, or scientific value for 16 year-olds lacks serious literary, artistic, political, or scientific value for 17 year-olds.

59. There is no speech that is harmful to a 16 year-old that is not also harmful to a 17 year-old.

III. COPA's AFFIRMATIVE DEFENSES DO NOT CURE ITS DEFICIENCIES.

A. In general

60. There are no age verification services or products available to Web sites that reliably verify the age of Internet users. There are no services or products that can effectively prevent access to Web sites by a minor.

61. There is a fee associated with all verification services identified in COPA, as well as others that claim to provide age verification. That fee applies any time a user attempts to access material on a Web site, even if there is no purchase. That fee will either be paid by the Web site or passed on to the users. As a result, Web sites such as Plaintiffs', which desire to provide free distribution of their information, will be prevented from doing so.

62. There is no effective way for content providers or Web site operators, including Plaintiffs, to determine the identity or the age of a user who is accessing or providing material through Web-based interactive fora such as discussion groups or chat rooms. The only way to ensure that material does not reach minors in any such interactive forum is to place all messages in all interactive fora behind screens accessible only to those users whose ages have been verified.

63. Because of the nature of the Web, COPA would require that users of any interactive forum provide a credit or debit card or sufficient personal information to pass through an age verification screen before entering the discussion – even if the discussion contains a wide range of speech that is not harmful to minors. There is no method by which the creators of an interactive forum could block access only to material that is "harmful to minors," but allow access to the remaining content, even if the overwhelming majority of that content is not harmful to minors.

64. The majority of Web users already refuse to register or provide any real personal information to Web sites if they have any alternative. Because age verification is costly and

difficult to use, and because requiring age verification would lead to a significant loss of users, many content providers will choose to self-censor rather than shoulder the larger burden of age verification.

65. Because of the way search engines work, credit card or other COPA screens will prevent web pages from being identified by search engines and, in turn, seen by users. Requiring use of age verification screens will have a negative effect on the operation of the Web. Search engines will, in particular, be affected by the widespread use of age verification screens and the placement of material behind such screens.

66. Because COPA covers a broad range of material, each Web site would need to create some organizational policy for determining what is harmful to minors and what is not. To comply with COPA, a content provider would be required to apportion some of its staff, or to hire new staff members, to review old and new content. This content includes all images, text, sounds and videos. These individuals must be well-versed in the legal definition or the organization's policy and have the authority to decide whether to place content into an "adult section."

67. There are no adult access code products, within the meaning of 42 U.S.C. §231(c)(A), that verify age.

68. There are no digital certificates, within the meaning of 42 U.S.C. §231(c)(B), that verify age.

69. There are no other "reasonable measures," within the meaning of 42 U.S.C. §231(c)(C), that verify age.

70. It is an affirmative defense to prosecution under COPA to restrict, in good faith, access by minors to material that is harmful to minors by requiring use of a debit card, including a non-reloadable prepaid card.

71. Minors have access to credit cards.

72. Minors have access to debit cards.

73. Minors have access to reloadable prepaid cards.

74. Minors have access to non-reloadable prepaid cards.

75. Web sites cannot choose to accept reloadable prepaid cards, but not accept non-reloadable prepaid cards.

B. Deterrence

76. Because the vast majority of content on the Web is available for free, most Web users will not provide credit cards or personal information simply to obtain access to Web content. Requiring users to provide a credit card or personal information before they can browse a Web page to determine what it offers will deter most users from ever accessing those pages; Web sites such as Plaintiffs' will lose many users as a result.

77. Requiring users to go through an age verification process would lead to a distinct loss in personal privacy. Many people wish to browse and access material privately and anonymously, whether viewing controversial or embarrassing content, reading about people they know, or considering purchases. Web users are especially not likely to provide a credit card or personal information to gain access to sensitive, personal, controversial or stigmatized content on the Web. As a result, many users who are not willing to access information non-anonymously will be deterred from accessing desired and necessary information, and Web sites such as Plaintiffs' will be deprived of the ability to provide this information to such users.

78. Although many users may risk transmitting their credit or debit card numbers over the Internet when they are making a purchase, many users are unlikely to take such a risk simply to access free content, particularly if that content is available on another site that does not require entry of that information.

79. Widespread adoption of policies requiring users to provide a credit card or debit card, or to otherwise provide detailed personal information to pass through an age verification screen, would create additional identity theft risks for Web users and increase people's fears and security concerns about using the Internet.

80. COPA's requirement that Web sites maintain the confidentiality of information submitted for purposes of age verification would not alleviate the deterrent effect of age verification on users, because users must still disclose the personal information and then rely on third parties, many of whom are unknown and have no actual person identified with them, to comply with the confidentiality requirement. The statute does not provide any recourse to users for confidentiality violations by Web sites. In fact, COPA explicitly grants immunity to content providers for any action taken to comply with COPA. 47 U.S.C. § 231(c)(2).

81. Requiring users to provide a credit card, debit card, adult access code, adult personal identification number or to otherwise go through an age verification screen before providing access to speech on the Web would completely bar many adults who lack such identification from access to information appropriate for them.

82. United States Web sites will also suffer and be put at a distinct disadvantage because foreign Web sites will not have to comply with COPA. Most likely, the vast majority of non-U.S. Web sites will ignore COPA. As a result, many users, inside and outside the U.S., will

gravitate toward non-U.S. sites that offer the same or similar information and services as U.S. Web sites, but that do not require the users to pass through an age verification screen.

C. Credit card and debit card verification

83. Credit card companies prohibit Web sites from claiming that use of a credit or debit card is an effective method of verifying age and prohibit Web sites from using credit or debit cards to verify age.

84. Many adults do not have credit or debit cards.

85. Many children have access to credit or debit cards. A significant percentage of minors have access to credit or debit cards with the express permission of their parents. A significant percentage of minors also have access to credit or debit cards without the knowledge or consent of their parents. The best estimate is that at least half of all children have such access. The percentage of 16 year-olds with access to payment cards is significantly higher than the percentage of 12 year-olds with access to payment cards.

86. Many issuing agencies market credit and debit cards to minors. Payment card companies increasingly market cards directly to minors. Currently, one of the main thrusts of credit card marketing in this country is to get payment cards into the hands of youth as early as possible. This marketing focus is still rather new, and in the coming years, it is likely that this focus will result in more and more minors having payment cards. Visa's "Visa Buxx" card is one example of a payment card that is specifically designed for and marketed to minors.

87. Many employers, such as McDonalds, pay minor employees by providing them with payment cards.

88. Payment card-based age verification schemes are not difficult to bypass. Minors can obtain payment card information to access "protected" areas of the Web through Web sites that offer those services.

89. There is no way for a merchant, such as a Web site, to know that a user is actually a minor. Merchants, including Web sites, that accept Visa or Mastercard credit cards or debit cards must honor all Visa or Mastercard credit cards or debit cards, including prepaid credit and debit cards.

90. Financial institutions will not process or verify a payment card in the absence of a financial transaction. Express policies of the payment card companies prohibit online merchants who sell content from processing transactions in the amount of zero dollars ($0). Verification by payment card will therefore be practically infeasible for all of the Plaintiffs and most other Web site operators and content providers covered by COPA who distribute their content and material for free.

91. The purpose of the payment card companies' processing systems is to process financial transactions or purchases. Those companies have regulations and policies designed to prevent their systems from being used for other, non-payment transaction-based purposes. Permitting zero-dollar transactions would threaten the system's capacity to process transactions, and would increase fraud by enabling criminals to enter numbers randomly into the system to identify active card numbers.

92. There is no reason for Web sites that do not sell anything – i.e., sites on which there is nothing for the user to purchase – to have relationships with any of the payment card companies.

93. Requiring use of a payment card to enter a site would impose a significant economic cost on Web entities. Payment card companies charge a fee every time a payment card is processed through their system.

94. Credit and verification charges must either be absorbed by the content provider or passed on to users. This cost will increase according to the number of visitors to a site. Many of the larger sites have well over a million unique visitors per day.

95. Credit cards are not commonly used for online transactions in Europe and Asia. The effect of COPA would be to divide the Web into two sections, one involving U.S. speakers who largely speak only to U.S. residents and another Web, composed of overseas sites who can speak to anyone including U.S. residents.

D. Data verification

96. A few companies offer non-payment card-based services and/or products that can be used in an attempt to verify age. These systems rely on a number of sources of public records, and some privately acquired information, in an attempt to verify age. Generally, these systems function by charging Web sites a per transaction fee in exchange for their checking personal data, supplied by the Web site's visitors, against a database of records either owned by or otherwise available to these systems. Before being given access to a Web site, a user will be required to provide specified personal information such as the person's name, last four digits of the social security number, home address, home telephone number, or driver's license number, on a Web form that is sent by the Web site to the verification system. The system will then check the data sent by the Web site against a database to see if the data matches that of an adult or a minor, or if the data cannot be verified, and then send the response to the Web site. Because these services essentially are checking data sources, rather than verifying the actual age of an

individual, these services are often referred to as "data verification systems," rather than "age verification systems."

97. These services are more accurate the more information and the more personal the information is that is provided. If the last four numbers of a social security number are provided, there is a much greater chance that the DVS company will be able to match the information to an individual than if basic information such as a name, street address, and ZIP code are required. If the latter is all that is requested, there is a much greater chance that the system will not be able to verify the data, and will not be able to determine if the user is an adult or a minor.

98. The web site operator decides what information to request from a visitor.

99. The more information provided, the higher the fee charged by the DVS will be. The fee charged to the Web site can climb upwards of fifty cents ($.50) per verification. There may also be other fees associated with using a DVS on top of the per transaction fees, such as setup fees.

100. DVS operators return one of three answers: data verified and not an adult; data verified and an adult; data not verified.

101. When COPA was first passed in 1998 and when this Court entered a preliminary injunction against enforcement of COPA in 1999, there were no data verification systems that accurately verified age. There are still no data verification systems that accurately verify age.

102. No data verification systems are able to verify accurately the age of everyone living in the United States. As a result, even adults living in the United States who submit valid and legitimate personal information to a DVS in order to access a Web site will often be denied access.

103. Existing data verification systems have an especially difficult time verifying the age of individuals who are between 17 and 21 years old. Because many individuals in the United States who are over 16 years old will not have their age verified by the existing data verification products, if Web sites such as Plaintiffs' utilize data verification products to comply with COPA, many adults will not be able to access those Web sites.

104. No data verification systems are able to verify accurately the age of anyone who lives outside of the United States unless those individuals have U.S. public records. Because many individuals living outside the United States who are over 16 years-old will not have their age verified by the existing data verification products, if Web sites such as Plaintiffs' utilize data verification products to comply with COPA, non-American adults will not be able to access those Web sites, and the audience for those Web sites will be limited solely to Americans even though there may be many people who might otherwise want to access the speech or content on the Web sites.

105. Because they often rely on basic personal information, such as a person's name and address, data verification systems are prone to abuse and can be circumvented with minimal effort by anyone, including minors, desiring to gain access to Web sites relying on data verification systems to verify age. That is, in part, because there is no way for a data verification system (or a Web site utilizing such a system) to verify that the person entering the personal information is actually the person to whom that information pertains. Nor is there any way for the person to whom that information does pertain to know that his or her information has been used because the DVS companies do not notify people when their information has been run through a check.

E. Digital Certificates

106. There are no digital certificates that can be used to comply with COPA.

F. Other reasonable alternatives

107. No other available or feasible options exist that allow Web sites to restrict access to certain material by minors while continuing to provide it to adults.

IV. COPA IS UNDERINCLUSIVE.

108. COPA's restrictions do not apply to email, chat, instant messaging, peer-to-peer file distribution networks, streaming video and audio content, voice-over-Internet telephone calls, or Internet television. COPA also does not cover speech utilizing the ftp protocol.

109. There is a significant amount of speech, including sexually explicit speech, that can be accessed using all of the forms of Internet speech listed in the prior paragraph. These modes of communication are used to distribute text, pictures, images, video, and audio content, among other things.

110. Millions of people, including a significant number of minors, use these forms of Internet speech on a regular basis. For example, approximately 90 percent of all Internet users send or receive email. 75 percent of online teens send instant messages, and it is estimated that about 50 percent do so on a daily basis. Hundreds of millions of files are distributed over peer-to-peer networks each week, and it is estimated that about 30 percent of all people downloading video and music files do so via peer-to-peer technology.

111. There is a significant amount of sexually explicit speech that can be accessed on the World Wide Web that is posted by sites that are not commercial.

112. There is a significant amount of sexually explicit speech on adult web sites on the World Wide Web that is hosted or registered overseas. A conservative estimate places 32 percent of adult membership sites and 58 percent of free adult websites outside the United States.

113. Adult web sites are migrating out of the United States, and free adult web sites are migrating at the highest rates. From 2001 to 2006, the United States' share of free adult web sites dropped from 60 percent to 42 percent. This is occurring due to U.S. regulations, low barriers to entry, and diffusion of Internet use.

114. Because adult Web sites that charge for viewing their content already require use of a credit or debit card for users to get access to their material, those Web sites will not be affected by COPA due to the statute's credit card affirmative defense. Because minors have access to credit and debit cards, the sexually explicit material on these Web sites will be available to minors even if COPA were to go into effect.

115. Much commercial pornography on the Web, especially adult videos and the higher quality images, is only available to those who pay for it.

116. Individuals wishing to evade COPA can do so by utilizing FTP instead of HTTP. The major browsers available today are capable of downloading files using the FTP protocol. For many file transfer or distribution applications, FTP is a viable alternative to HTTP. It is relatively easy to use FTP instead of HTTP, and the necessary software is available for free.

117. Speech that is communicated over email is not covered by COPA and cannot be prosecuted under COPA.

118. Speech that is communicated over peer-to-peer networks is not covered by COPA and cannot be prosecuted under COPA.

119. Speech that is communicated via chat is not covered by COPA and cannot be prosecuted under COPA.

120. Speech that is communicated via instant messaging is not covered by COPA and cannot be prosecuted under COPA.

121. Speech that is communicated via streaming video and audio cannot be prosecuted under COPA.

122. Speech that is communicated via online television is not covered by COPA and cannot be prosecuted under COPA.

123. Speech that is communicated via newsgroups, such as USENET, is not covered by COPA and cannot be prosecuted under COPA.

124. All of the forms of Internet communications listed in the prior eight paragraphs can be used to communicate images as well as text.

125. All of the forms of Internet communications listed in the prior eight paragraphs can be blocked, in whole or selectively, by Internet content filters.

V. THERE ARE A NUMBER OF LESS RESTRICTIVE ALTERNATIVES TO COPA THAT ARE AT LEAST AS EFFECTIVE AS COPA.

A. Internet Content Filters

(1) Summary of Internet Content Filters

126. Internet service providers ("ISPs") and commercial online services like America Online provide parents with a wide range of mechanisms that parents can use to prevent their children from accessing material online that they do not want their children to view. Parents can tailor these services to their own values and to the age and maturity of their child. These services reach, and block, speech that is posted overseas, posted on non-commercial sites, or available in non-Web-based mediums, such as email, instant messaging, chat, newsgroups, peer-to-peer file sharing, and any other formats other than http. They can be used to block all speech in all interactive fora.

127. Similar services and software are offered by numerous private software companies.

128. Parents and other online users can use filtering programs, also known as user-based blocking programs, to restrict access to sexually explicit content. These programs allow users, among other things, to block access to sexually explicit web pages, to prevent children from giving personal information to strangers by e-mail or in chat rooms, and to keep a log of all online activity that occurs on the home computer.

129. Internet content filters are computer programs designed to restrict access to certain types of material on the Internet. They are used frequently by employers to restrict the Internet access of their employees, and by schools, libraries, and parents to restrict the Internet access of children.

130. Internet content filters can be programmed or configured in a variety of different ways. They can be set up to restrict materials based on the type of content they contain (adult material, information about drugs, etc.), the presence of particular words, the address of the Web site, or the Internet protocol or application used (World Wide Web, email, instant message, peer-to-peer, etc.). Some filters can also restrict access based on time of day, day of week, how long the computer has been connected to the Internet, or which user is logged onto a computer.

131. Some filtering programs offer only a small number of settings, while others are highly customizable, allowing a parent or other administrator to make detailed decisions about what to allow and what to block.

132. Some Internet content filters are built into the services provided by ISPs; a family that subscribes to an ISP that provides filtering services can usually take advantage of these services without installing additional software on their computer. Filters may also be built into cable modems, wireless access points, and other Internet access devices. Filters will also soon be

available as part of Microsoft's new operating system, meaning that all computers that come with Microsoft's operating system installed will have built-in parental control features.

(2) Methodology of Internet Content Filters

133. Filters enable parents and other to control access to the Internet through a variety of different mechanisms.

134. Some filters use "black lists" to filter out content. Black lists are lists of Web site addresses (URLs) or Internet Protocol (IP) addresses that a filtering company has determined point to content that contains the type of materials their filter is designed to block. Some companies offer black lists that are very extensive, containing millions of Web sites, many of which are published in languages other than English.

135. Black lists may be compiled in a variety of ways. A filtering company may use an automated Web crawler to identify new URLs that may contain content that should be blocked. They may have human employees search for additional sites. They may also run frequent search engine queries using search terms likely to result in content that should be blocked in order to identify new Web sites containing such content. Filtering companies do this because a significant proportion of people find Internet content today through search engines, and mimicking these searches allows the companies to identify the sites that people are most likely to see and access. In addition, some companies review industry lists of popular Web sites, or "most viewed" Web sites, to ensure that their products cover those sites that Internet users are most likely to attempt to access. They may also collect reports of URLs that should or should not be blocked from their users, from their business partners, or from governmental entities. Finally, filtering companies may purchase or otherwise acquire lists of Web sites from other entities, including search engines, to supplement the sites they have independently located.

136. Once the URLs are identified, filtering companies may use an automated system to evaluate the URLs and to decide which should be put on the black list, or they may have their employees check those URLs to confirm that they meet the blocking criteria. Some companies require human review of every site included on their content lists to ensure accuracy. When filtering companies identify URLs that meet their blocking criteria, they may set up their black lists to block just one particular Web page, a section of a Web site, or the entire Web site.

137. Most filtering products that use black lists contain mechanisms for frequently updating these lists and providing those updates to their users. Many of these updates are done automatically, without requiring the user to do anything.

138. In addition to their own black and white lists, many filtering products give parents or administrators the option of creating customized black or white lists. For example, AOL allows parents to specify URLs that they want to be blocked or allowed, regardless of the default settings for a particular age category. Many filters allow these customized lists to be created for multiple users, on a user-by-user basis, enabling a parent who has a child who is 16 years old and a child who is 6 years old to create separate customized black lists and white lists for each child. In addition, if parents believe their child is mature enough to see some, but not all, sites of a particular type, they can set their filter accordingly.

139. Several of the filtering products have divided up their lists into multiple categories; parents can decide if they want to block or allow Web sites within each such category. These categories cover far more than just sexually explicit material, enabling parents to restrict their children's access to whatever kinds of content they choose, not just sexually explicit materials. For example, in addition to "adult" content, many of the filters have categories for drugs, weapons, violence, hate speech, and other subjects which some parents might find inappropriate

for their children. Some companies that offer multiple content categories allow parents to place a particular site within whichever category they choose, even if this is not the default setting, enabling parents to change decisions made by the filtering company if the parent disagrees with the company's categorization.

140. In addition to relying on black lists and white lists, some filters also use "key words" or other real-time, dynamic filtering techniques to limit access to certain Web pages. Filtering companies may compile lists of words and phrases associated with content that should be blocked, even if the page has not previously been categorized. Some products just remove those words from the page, while others block the entire Web page that contains these words or phrases. They may also develop templates that provide additional context and prevent over blocking – for example, that block the word "breast" when used in combination with the word "sexy," but not when used in combination with the words "chicken" or "cancer."

141. Some filters also use artificial intelligence or machine-learning techniques to teach their software to determine whether content should be blocked if it is not already on a list. Every time the software encounters a new Web page, the filter can analyze the content and determine how similar it is to the examples it has seen in the past and therefore whether or not it should be blocked. Much like other similar software, filtering products use statistical pattern recognition techniques to identify features of acceptable and unacceptable Web pages, which may include combinations of words, links, formatting, or other features.

142. Some filters apply these types of real-time techniques to image blocking, just as they do to text blocking. Filtering companies can use artificial intelligence or machine-learning techniques to "teach" their filters which images should be blocked. They can also use computer vision techniques to identify body parts or other visual images that should be blocked. Although

image-filtering techniques by themselves tend to be less accurate than text filtering techniques, image filtering can be effective when used in combination with text filtering techniques – for example, examining both images and the textual image captions to determine whether content should be blocked. Indeed, studies done by one of the filtering companies in connection with their mobile filtering product indicate that their image filter is 87 percent accurate if there is no text whatsoever on a page, and when the image filter is combined with their text-based product, the filter is 99.48 percent accurate.

143. The metadata, or hidden text tags, attached to Web sites also help filters to find and block inappropriate images. For example, if there is an image on a page, but no visible text or caption, and the metadata identifies it as adult material, filtering products will still locate the page and filter it according to its content. Metadata is used to allow search engines to locate and recognize sites easily. Web site developers usually include metadata to increase the chances that search engines will include their site near the top of a list of search results. Because filtering companies use search engines to find potentially inappropriate sites, they are likely to find the large majority of sites with inappropriate images that users might actually see.

144. Many filters combine and layer several of these different filtering techniques in order to increase the effectiveness and accuracy of their products. For example, Looksmart's product, NetNanny, and AOL's mature teen filter make use of black lists, white lists, and dynamic, real-time filtering. By combining these different approaches, filtering products have become increasingly effective.

(3) Non-content filtering aspects of Filtering Products

145. In addition to their content filtering features, filtering products have a number of additional tools to help parents control their children's Internet activities. Other tools available

to parents include monitoring and reporting features that allow supervising adults to know which sites a minor has visited and what other types of activities a minor has engaged in online. AOL, for example, offers a feature called AOL Guardian, which provides a parent with a report indicating which Web sites a child visited, which sites were blocked, the number of emails and instant messages a child sent, and to whom a child sent email or instant messages. Surfcontrol similarly provides parents with reports of the sites a child has visited, as well as those that were blocked; their product also has the ability simply to monitor a child's activity without actually blocking anything, if a parent prefers that option. Contentwatch has a feature that permits parents to monitor their child's Internet activities remotely, for example, while they are at work.

146. Several filtering products also provide parents with the option of having a warning appear before a child's access to certain material is permitted, rather than having the material blocked. The child will then have the option of going into the site, if he or she believes it is appropriate to view, or not going into the site, if it is deemed to be inappropriate or undesired.

147. Many filtering programs also offer parents the ability to restrict the times of day that a child can use the Internet, or to control the total amount of time in a given day that a child may use it. Filtering software can similarly restrict Internet access by days of the week, making it possible for parents to make sure that their children only access the Internet when an adult is home to supervise.

148. Filtering programs can also be used by parents to prevent their children from having any access to parts of the Internet other than the Web, and to certain Internet applications which parents do not want their children to have any access to, such as e-mail, chat, instant messaging, newsgroups, message boards, and peer-to-peer file sharing. Some products also provide parents with the option of providing limited access to these Internet applications. For example, instant

messaging and e-mail may be permitted, but some of the products will only permit the sending and receiving of messages from certain authorized individuals, and will block e-mails or instant messages containing inappropriate words. Filtering programs can also completely prevent children from entering or using chat rooms, or they can merely filter out any inappropriate words that come up during a chat session. Many of the products can also be set up to prevent children from inadvertently or intentionally sending out personal information, such as a home address or telephone number, and to block children from receiving downloads, attachments, or file transfers through any means.

(4) Filters Are Widely Available

149. Filters are widely available and easy to obtain. Besides the numerous filtering products sold directly to consumers, filters are also available through ISPs. Eight of the top ten-most used ISPs offer content filtering for free; the other two ISPs (Verizon and United Online) offer it for rates of just $4.95 and $1.95 per month respectively.

150. Estimates of the major ISP's market shares are:

ISP	Subscribers (in millions)	Market Share
1) America Online	18.6	20.1%
2) Comcast	9.0	9.7%
3) SBC (AT&T)	7.4	8.0%
4) Verizon	5.7	6.2%
5) Road Runner	5.4	5.8%
6) Earthlink	5.3	5.8%
7) BellSouth	3.1	3.4%
8) Cox	3.1	3.3%
9) United Online	2.8	3.0%
10) Charter	2.3	2.5%

151. Filters will also soon be pre-installed in computers using Microsoft's new operating system. Microsoft has announced plans to launch a new operating system called Vista by

January 2007, which will contain Internet content filters, along with other access control tools for parents like time management, activity logging, and the ability to block or restrict children's access to online games. Anyone using this new operating system will automatically have access to these filtering tools. Vista will be compatible with third-party content filters, meaning that other companies will be able to classify content and provide those classifications in a format that will be readable by the Vista parental controls, enabling parents to configure third-party filters through the Vista control panel. Because the vast majority of computers come pre-loaded with Microsoft's current operating system, Windows, the vast majority of computers will have built-in, free, compatible filters.

152. Microsoft has also announced that for those computers not using the new operating system, it will soon make a free content filter available as part of their Windows Live offering. Once the Windows Live parental controls are released, anyone with a computer running Windows XP will be able to download and use free parental controls software to filter content accessed with any Web browser.

(5) Internet Content Filters are Easy to Use

153. Filtering programs are easy to install, configure, and use.

154. Almost all parents will be able to install filtering products and use them by selecting from one of their standard settings. Many filters, such as AOL Parental Controls and Cybersitter 9.0, have user interfaces that are quite easy to use and make it easy for users to create customized settings.

155. Installation and initial configuration are areas that always pose some challenges for software users, and it is quite difficult to design software that absolutely everyone will find easy to use. Filtering software is no more difficult to install or use than other software that is widely

used every day. For example, programs like Microsoft Word offer many options and settings that users have to navigate in order to use them effectively, and millions of people use such software.

156. Although there were occasional user complaints about latency (delay) with early-version filtering products, latency is much less of an issue with today's filtering products. Existing filters do not usually cause any significant or noticeable delays. The amount of time it typically takes filters to look URLs up in black lists and white lists is generally imperceptible. Even real-time filtering should take only slightly longer than the amount of time it normally takes to load a web page – i.e., milliseconds. That is in part because the products have improved and eliminated most of those issues, and also because more and more Internet users are moving to higher speed broadband connections.

157. Installation problems and other technical issues, like compatibility, are disappearing as more and more people use filtering that is bundled with their ISP service or provided on the network rather than on each individual personal computer. In addition, many filtering products are now bundled together with other software, such as a larger security suite. As a result of these developments, customers no longer need to install stand-alone programs on their personal computers, and bundled filters are by definition compatible with a user's Internet service, along with any other security services offered through that provider. Windows Live and Windows Vista will similarly ease technical problems, because they will contain filters that, as part of the operating systems themselves, will work with any other program that is designed to be compatible with Windows.

(6) Filters Cover More Speech than COPA

158. Even if COPA had been drafted differently to cover overseas Websites, COPA cannot be enforced against a speaker who is not subject to U.S. law either because he or she is outside the jurisdiction or for any other reason.

159. Filtering products can be used by parents to block speech on the Web no matter where the Web sites are located.

160. Filtering products can be used by parents to block both non-commercial and commercial Web sites.

161. Filtering products can be used by parents to block harmful to minors material that is paid for or free.

162. Filtering products can be used by parents to block material that is distributed on the Web and on the other widely used parts of the Internet through protocols other than http. Specifically, filters can be used to block, among other things, e-mail, chat, instant messaging, peer-to-peer file sharing, newsgroups, and Internet television.

163. Filtering products will also better protect children and make the Internet a safer place for children than COPA because they reach a far broader range of content than COPA, enabling parents to restrict their children's access to whatever kinds of content they choose, not just sexually explicit materials. For example, many products include categories like Violence, Drugs, Alcohol and Tobacco, Weapons, and Criminal Skills.

164. Filtering products also provide a more flexible solution than COPA because filtering products can be tailored to meet the individual values, desires, and needs of Internet users and/or their parents, and the age and maturity of a child. The wide range of user-based filtering options that are available at low or no cost permits parents and families to choose those options which

are most consistent with their own family values and the circumstances of their children, including the age and maturity of each child, not the values of some other family or community.

165. Filtering products offer complete flexibility in that parents can turn them off any time they do not want to block material for themselves, other adults, or for their children. As a result, the potential for overblocking problems is greatly lessened in the context of voluntary parent-initiated filtering.

(7) Effectiveness Of Filtering Products

166. The FBI, which is an agent of Defendant, uses an Internet content filter for most of its computers which blocks access to sexually explicit material. The FBI is satisfied with the operation and effectiveness of the filter and has received few complaints about underblocking.

167. The Bureau of Alcohol, Tobacco, and Firearms, which is an agent of Defendant, uses an Internet content filter for most of its computers which blocks access to sexually explicit material. The Bureau is satisfied with the operation and effectiveness of the filter and has received few complaints about underblocking.

168. The Federal Bureau of Prisons, which is an agent of Defendant, uses an Internet content filter for most of its computers which blocks access to sexually explicit material. The Bureau is satisfied with the operation and effectiveness of the filter and has received few complaints about underblocking.

169. Filtering products can be an effective tool to prevent children from accessing material deemed inappropriate for them, especially pornographic material. Although they are not perfect, filtering products block the vast majority of the material on the Web that is sexually explicit and that might be considered harmful to minors.

170. Individual filtering products vary in how effective they are at both accurately blocking intended material and not inadvertently blocking appropriate material. The better products are very good at blocking intended material and have very low rates of erroneously blocking material.

171. Filters can be made more restrictive or less restrictive and, thus, can block more or less material, depending on the individual desires of parents. The more willing a parent is to have some material inadvertently blocked, the more effective the product will be at blocking virtually all sexually explicit material. If a parent wants to make sure that his or her child does not have access to absolutely any sexually explicit material, the parent can set the filtering product accordingly and, in doing so, can make sure that there is an extremely low chance – likely less than 1% -- that such material will be accessible.

172. Filters work especially well at blocking the most popular Web sites and the Web sites that are most likely to be accessed by a minor. For example, it is highly likely that every Web site that comes up in the first 50 results of a search engine query for "hard core porn" will be blocked by filtering products. Looksmart, for example, blocks the first 50 results for Google and Yahoo searches for "hard core porn."

173. The emergence and widespread popularity of search engines, which have led most Internet users to go to sites through described search engine links rather than typing a URL, combined with the Misleading Domain Name statute, has made it much less likely that a child will inadvertently access sexually explicit material if a filter is not being used, and even less likely if a filter is being used.

174. Many search engines, including Google, provide a filtering feature for parents to use to block results that contain material not appropriate for children.

175. Many studies have been done to measure the effectiveness of various Internet content filtering products. The exact results of these studies often differ because of differences in their evaluation criteria and methodology. Evaluations of filter effectiveness usually focus on how accurate filters are at distinguishing between content that should and should not be blocked. "Under blocking" occurs when a filter fails to block content that is supposed to be blocked. "Over blocking" occurs when a filter blocks content that is not supposed to be blocked.

176. Although test results vary, most reports indicate that the better filters have under block rates of less than 10 percent, with some having under block rates of less than 1 percent or in the 1-2 percent range. These filters typically have over block rates that are lower than their under block rates when configured with settings designed for older children.

177. Exact percentages will vary depending on the study's methodology and the Web sites tested. As expected, studies show that many filtering products are very accurate in connection with the most widely viewed or accessed sources of sexually explicit material. For that material, most products will have an underblock rate of less than 5 percent, and an even smaller overblock rate. Simply testing for random Web sites, that may never have been viewed by anyone in the United States, let alone minors, may lead to slightly higher underblock or overblock rates, but generally, several products will still have underblock rates of less than 10 percent .

178. Studies have also shown that while filtering products block the vast majority of all material potentially inappropriate for children, the products are even better at blocking material that is clearly pornography and erotica, and they will block virtually all such material.

179. Two separate reports commissioned by Congress – from the Commission on Child Online Protection and the National Research Council – have confirmed that content filters can be effective at preventing minors from accessing harmful materials online. The COPA Commission

report notes that filters can be effective in directly blocking global content, as well as content in newsgroups, email, and chat rooms. It points out that content filters are "flexible" and can be customized based on family choice. It also notes the existence and value of time management and logging features, particularly for encouraging parental involvement and influencing children's activities online. Overall, it points out that "voluntary approaches provide powerful technologies for families."

180. The National Research Council Report concurs, stating that "filters can be highly effective in reducing the exposure of minors to inappropriate content," and "it is helpful to regard such filtering as 'training wheels' for children on the Internet as they learn to make good decisions about what materials are and are not appropriate for their consumption"

181. Filtering products have improved over time and are now more effective than ever before, both in blocking intended material and in not blocking unintended material.

182. Filtering products today cover more speech than ever before, in more languages, and offer more options to parents to customize the products to fit the individual circumstances of their families and children.

183. A major development for filtering products is that many products now provide multiple layers of filtering. Whereas filters once only relied on blacklists or whitelists, many of today's products utilize blacklists, whitelists, and real-time, dynamic filtering to catch any inappropriate sites that have not previously been classified by the product. This multi-layered approach has increased the effectiveness of content filters and enables parents to block much more material if that is desired.

184. There is a high level of competition in the field of Internet content filtering. That factor, along with the development of new technologies, has caused the products to improve over

time. Given that consumer demand has not diminished, it is likely that the products will continue to improve and become even more effective over time.

185. Parents using filters are satisfied with their filtering products, and many believe the products are outperforming their expectations. For example, a study done for AOL found that 85 percent of parents are satisfied with their AOL Parental Controls products, and that 87 percent find them easy to use.

186. Many government agencies use Internet content filters on their computers. Testimony from the Department of Justice itself confirms that filtering products work, and that Internet users are very satisfied with the way they work.

187. Libraries also widely employ Internet filters. Despite personal views that full access to information is preferable, many librarians are very satisfied with the products and the way they work. As one example, in a 2003 article, Hampton Auld, a Virginia librarian, noted that during the first seventeen months of filtering in his library system, 2.4 million patrons surfed the Web and there were a mere 38 requests to unblock and 38 requests to block Web sites.

188. Schools similarly use filters to make sure that their students do not encounter inappropriate material. Students are regularly testing the effectiveness of filters in real-world setting, by accessing thousands of Web sites per week from their school or school library computers. Many schools are satisfied with the protection and services offered by content filters.

189. One of the features of filtering programs that adds to their effectiveness is that they have built-in mechanisms to prevent children from circumventing them, including password protection and devices to prevent children from uninstalling the product or adjusting a computer's clock to outsmart time settings. Some products have a tamper detection feature, by

which they can detect when someone is trying to uninstall or disable the product, and then cut off Internet access altogether until it has been properly reconfigured.

190. Very few minors have the technical ability and expertise necessary to circumvent filtering products either by disabling the product on the actual computer or by accessing the Web through a proxy or intermediary computer to avoid a filter on the minor's computer.

191. Accessing the Web through a proxy or intermediary computer will not enable a minor to avoid a filtering product that analyzes the content of the Web page requested, in addition to where the page is coming from. Any product that contains a real-time, dynamic filtering component cannot be avoided by use of a proxy, whether the filter is located on the network or on the user's computer.

192. Filtering product companies actively search the Internet to identify any material that is posted online in an attempt to provide means to circumvent filtering products, and take steps to ensure that such material is blocked in the first place and cannot be used to circumvent their products.

193. Any theoretical problem with circumvention is eliminated by filtering products that are provided by ISPs, the vast majority of today's filters. Because ISP-bundled filters are run on the ISP's network, and are not located on the user's computer, there is no way for users to tamper with or somehow avoid the software.

194. The popularity of laptop computers is of no consequence to filtering products because they work on both desktop and laptop computers. Thus, if filtering software is installed on a laptop computer, it can filter Internet content wherever the computer is used, even if a child takes it outside the home.

195. Filtering products are also designed to work if a family has more than one computer, as they can be installed on multiple computers in a home.

(8) Filtering Products Are Widely Used By Parents

196. Many people are using the parental control tools offered by content filtering products. Although the exact number of people using filters is difficult to determine, the most recent and most reliable studies have consistently found that about 55 percent of parents with Internet access at home are using filters. That figure shows that there has been a significant increase in filter use by parents – about a 65 percent increase – from earlier studies conducted as recently as 2000.

197. It is not known why some families do not use filters. Some parents may have decided that they are unnecessary or not desired (because they trust their children or for some other reason), some may be unaware of filters, or others may not use them for other reasons such as cost or (real or perceived) difficulty of use.

198. Filtering products are essentially one type of security software for use by computer owners. Statistics show that other highly effective security software products, such as anti-virus software, are not used by all computer owners for a variety of similar reasons. The percentage of users utilizing filtering products is not unexpected and is in fact a higher percentage of use than many analysts would have expected.

199. Filtering products are widely used in most schools and libraries. Any school or library that receives federal funding for providing Internet access is required by a separate federal law, 21 U.S.C. § 9134; 47 U.S.C. § 254(h), to have filters installed and operating on all computers that are accessible by minors.

B. Internet Content Filters Used on New Technologies

200. Content from the Internet is now capable of being viewed on devices other than traditional personal computers. Examples include mobile devices such as mobile phones, personal digital assistants ("PDAs") such as the Blackberry, portable audio/video players such as the iPod, and game consoles such as the XBox or PlayStation. Many of these devices are essentially computers, packaged differently, and with differing user interfaces.

201. Although many devices are now capable of accessing the Internet, a very small percentage of individuals with such devices are actually using them to access the Internet. The percentage is even lower for the number of minors accessing the Internet through these devices. For those individuals who are using new devices to access the Internet, by far the most common use is to access email; because of both speed and cost issues, a significantly lower percentage of people use alternative devices to browse the Web.

202. Content filtering technology can be used on these alternative, non-PC devices, and there are no fundamental barriers to the feasibility of content filtering on the devices. It is possible to provide the same type and quality of content filtering for such devices as for ordinary computers.

203. Some alternative devices, such as certain PDAs and portable music players like the iPod, cannot receive content directly over the Internet, but can only receive it via a wired connection to a personal computer, after the content has been downloaded to the personal computer first. For these devices, the content will already have been subjected to the personal computer's Internet content filter, if the user has chosen to use a filtering product, so an additional filtering product for these devices is not necessary.

204. Filtering technology can be implemented for users of other alternative devices in several ways. One approach is to perform content filtering in the network, not on the device

itself, much as is done for most ISP-based filters for personal computers. In this approach, equipment run by the network provider (e.g., the cellular network for a mobile phone) would observe, inspect, and filter network traffic in transit between the alternative device and the rest of the Internet.

205. Another approach is to run filtering software on the device itself. Devices such as mobile phones are really just small computers, which are capable of running the same types of software applications that desktop computers can run. The creator of a filtering program for desktop computers can simply take that program and modify it slightly so that it works on an alternative device.

206. Some alternative devices have less memory or slower processors than desktop computers. Less capable devices may have difficulty running some application programs. Due to the rapid and fairly predictable improvements in the capacity of memories and discs and the speed of processors, this state of affairs will only be temporary, and it is very likely that in the near future, almost all alternative devices will be able to run almost all applications that are used on personal computers today, including anti-virus software and content filtering software.

207. Yet another approach to implementing filtering for alternative devices is to pass the Internet content through a filter computer before delivering it to the end user's device, using what is called an HTTP proxy. Standard Web browsers support an option to use an HTTP proxy. When a proxy is in use, and the browser needs to retrieve a file via HTTP, the browser does not request the file directly from the server that is offering it. Instead, the browser contacts the proxy and tells the proxy the URL of the file the browser wants. The proxy then contacts the server, retrieves the designated file, and passes the file back to the browser. Because the proxy handles

every file (i.e., every page, image, etc.) that the browser gets, the proxy can filter the files to remove specified material, such as harmful to minors material.

208. Accessing the Web via a proxy, rather than accessing servers directly, makes no material difference in the amount of memory, computational power, or other resources that a mobile device will use. There is no noticeable difference for the user.

209. Mobile devices can, and often do, use HTTP proxies.The filtering proxy can be a computer (or bank of computers) anywhere on the Internet – it might be provided by a mobile phone company, by a filtering company, or by anyone else.

210. All of these filtering methods for alternative Internet access devices can be implemented transparently to the user, so the user's experience of using the device would be the same as it would be if the filter were not present (except for the unavailability of filtered content). The user interface for enabling, disabling, and controlling the filter could be essentially the same as on an ordinary computer.

211. Several vendors, including large, experienced software companies, currently offer content filtering products for alternative devices. Examples include products offered by Ace*comm, Flash Networks, Bytemobile, Blue Coat, BCGI, Cisco, PureSight, Syniverse, and RuleSpace, to name a few.

212. The companies that provide filtering products for traditional computers could also relatively easily modify their products for use on alternative devices. Many do not currently have products available for use on alternative devices because, given the recent emergence of such devices, there has not yet been a market demand for such products. Several of these companies are now considering whether to provide such a product, and once the demand is there, they are likely to provide such a filtering product.

213. Several major mobile phone carriers, including Cingular, Sprint-Nextel, and Alltel, are offering parental controls features, including some content filtering, to enable parents to control their children's access to the Internet. These tools enable parents so desiring to, among other things, limit the Web content accessible through the phones to pre-selected, child friendly material, and prevent their children from using chat rooms, instant messaging, text messaging, email, purchasing any file downloads or having any access to the Internet at all. By reviewing their monthly billing statements, parents can also monitor whether their child is accessing the Internet and, if the child has purchased anything, find out details about what is being purchased.

214. Blue Coat's content filtering product is being used by the mobile operator Vodafone for its customers. Byetemobile's filtering product is being used by T-Mobile UK. Although no U.S.-based carriers are yet providing the same content filtering that is currently available for personal computers, once the demand for such filtering emerges, it is highly likely that such products will be provided.

215. Ace*Comm's Parent Patrol product allows parents to impose usage restrictions on their children's cell phones, including restrictions based on time-of-day, service, specific phone numbers, and total talk time. Parent Patrol also includes content filtering. Ace*Comm has a contract with a North American carrier for deployment of elements of its Parent Patrol Product.

216. The major U.S. cell phone carriers have agreed to abide by industry guidelines concerning Internet access and wireless content. Those guidelines require the carriers, among other things, to: (1) classify content into at least two categories – content available for all users and restricted content available for those over 18 years-old or those whose parents have specifically authorized access; (2) not provide access to restricted content until the carrier has deployed controls to restrict access to such material; (3) provide controls to restrict access to

restricted content; and (4) consistent with each company's business plans, provide users with access to content filters that can restrict all Internet content not previously classified by the carrier.

217. Parents who are especially concerned about their children accessing inappropriate content through their cell phones can take advantage of a different technology: cell phones designed specifically for children.

C. Other Less Restrictive Alternatives

(1) Prosecute Existing Laws: Obscenity Prosecutions

218. Existing laws make it illegal to distribute material over the Internet that constitutes obscenity, 18 U.S.C. § 71, or child pornography, 18 U.S.C. §§ 2251-60.

219. Despite repeated requests from private citizens, politicians, interest groups and others, there have been very few prosecutions for obscenity over the past ten years.

220. From 2000 to 2005, Defendant initiated fewer than 10 prosecutions for obscenity which were not also linked to charges of child pornography, travel in interstate commerce to engage in sex with a minor, or attempting to transfer obscene material to a minor.

221. There have been fewer than 10 such prosecutions since 2005.

222. Much of the material that might be considered harmful to minors and prosecutable under COPA would also be considered obscene and is therefore already prosecutable under existing laws.

223. The government's interest in protecting children from harmful to minors material could be addressed through vigorous enforcement of other existing criminal statutes.

(2) Misleading Domain Name Prosecutions

224. Existing law prohibits the use of misleading domain names by Web sites. 18 U.S.C. § 2252B. That law is designed to prevent Web site owners from disguising pornographic Web sites in a way likely to cause uninterested persons to visit them.

225. Despite repeated requests from private citizens, politicians, interest groups and others, there have been, at most, only a very few prosecutions under this statute. In fact, there has only been one conviction under the statute since it was enacted. (News articles, case conviction)

226. Defendant has initiated less than 10 prosecutions under the Misleading Domain Names statute, 18 U.S.C. § 2252B.

227. More vigorous prosecution of this statute would decrease the frequency with which minors inadvertently encounter unwanted sexually explicit material on the Internet.

(3) Congress Could Enact A More Limited, More Narrowly Tailored Statute.

(a) The statute could apply to images only.

228. COPA's prohibition on material that is harmful to minors applies to any "communication, picture, image, graphic image file, article, recording, writing, or other matter." 47 U.S.C. § 231(e)(6). COPA therefore applies to written material with no images, and to audio recordings and other materials with no images.

229. Congress could enact a statute that only applies to material containing harmful to minors images or pictures. Such a statute would be less restrictive than COPA.

(b) The statute could impose only civil penalties.

230. COPA imposes significant criminal penalties, including imprisonment, in addition to severe civil penalties for violation of the statute. 42 U.S.C. § 231(a)(1).

231. Congress could enact a statute that provides only for civil penalties, and does not subject Web sites to potential criminal liability. Such a statute would be less restrictive than COPA.

(c) The Statute Could Require Labeling of Harmful to Minors Material

232. COPA imposes severe criminal and civil penalties for distributing material that is harmful to minors over the Web. Congress could enact a statute that permits the distribution of such material, but instead requires Web site operators to include a rating, label, or code on the Web site that makes clear that harmful to minors material is available on the Web site. Such a rating, label or code could be placed on the initial, home page of the site or in the hidden text, the metadata, associated with the site.

233. A proposal to enact exactly this sort of statute has been endorsed by the current administration and has been introduced in Congress. The Department of Justice has issued public statements backing such a proposal as a means of protecting children.

234. Requiring Web sites to include a harmful to minors rating, label or code would make filtering products even more effective and accurate at blocking harmful to minors material.

(d) The statute could require filtering products to contain a Harmful to Minors category.

235. In a separate statutory provision not challenged here, Congress has required that ISPs and online service providers make information about parental control tools such as filtering products available to their customers. Congress could enact a statute that requires all companies or individuals distributing Internet content filtering products to include a harmful to minors category for parents to use to block material covered by COPA, and Congress could provide specific, express guidance as to what sorts of materials should be included in that category.

(e) Government-Provided List of Harmful to Minors Web Sites.

236. Congress could enact a statute requiring the Department of Justice or another governmental entity to compile and maintain a list of Web sites that contain material that is harmful to minors. Alternatively, the Department of Justice could do so on its own initiative.

237. Such a statute (or action) would provide filtering product companies with the ability accurately to block absolutely all speech that the government believes is harmful to minors. It would also provide parents and other entities with information about the types of material that are on the Web in order to assist parents in determining what protections, if any, are necessary for their children depending on their individual values and circumstances.

238. Filtering product companies could also be forced, by statute, to include a harmful to minor category in their products that contains all of the Web sites included on the government's list. The State of Utah recently passed a law requiring its Attorney General compile an "adult content registry," a list of harmful to minors but non-obscene URLs. The law requires ISPs, at customer request, to block access to URLs on the adult content registry.

239. The filtering product companies would accept a governmentally-created list of inappropriate sites; in fact, many have already testified that they would almost certainly comply with any request from a governmental entity to include specific sites on their lists.

(4) Education: Encourage and fund educational efforts

240. Teaching children how to use the Internet is an effective method of ensuring their protection.

241. Congress could encourage additional educational efforts through pilot programs and funding.

(5) Other Parental Measures

242. Non-content filtering tools offered by filtering companies as well other parental measures are very valuable and effective in helping parents control their children's Internet activities.

243. Parents can utilize other measures to monitor and guide their children's use of the Internet. This can include placing the computer in a family room where its use can be observed, establishing rules for use of the computer, monitoring the child's time on the computer, tracking the web sites to which the child goes.

(6) Funding of independent rating systems

244. Congress could fund an independent organization to rate web sites and make such ratings available to parents for their use.

C. Defendant's Statement of Facts that Are in Dispute

I. INTRODUCTION

1. None of the plaintiffs has standing to maintain this action.

2. None of the plaintiffs has a credible fear of prosecution under COPA.

3. The defendant has a compelling interest in protecting minors from exposure to sexually explicit material on the World Wide Web.

4. Sexually explicit material is commonly found on the World Wide Web.

5. Sexually explicit material is widely accessible by minors on the World Wide Web.

6. The exposure to pornography has harmful effects on minors.

7. Internet content filtering software cannot completely protect minors from exposure to sexually explicit material on the World Wide Web.

8. Filtering software tends to underblock sexually explicit material. Thus, minors will be exposed to sexually explicit material on the World Wide Web even if filtering software is used.

9. Filtering software also tends to overblock non-sexually explicit material. Software that is more effective at avoiding the underblocking of sexually explicit material also tends to be less effective at avoiding the overblocking of sexually explicit material. Thus, in the absence of the solution offered by COPA, parents are left with the Hobson's choice of allowing their children to be exposed to sexually explicit material or of cutting off their children's access to a significant portion of other materials on the World Wide Web.

10. Filtering software relies on a formal analysis of the text of a web page to determine whether that page is sexually explicit. No automated system, however, is capable of analyzing the formal features of text with the accuracy needed to ensure that filtering software will be effective.

11. These limitations of automated systems are inherent in any attempt to classify text on a purely formal basis. Thus, no text-based filtering system will ever be able to minimize both the underblocking of sexually explicit material and the overblocking of non-sexually explicit material.

12. Filtering software can be effective, only if parents actually use it. In fact, however, at most 55 percent of households with minor children, and more likely only 40 percent of those households, use filtering software.

13. Many families are deterred from using filtering software because they have found the products to be too complex to use, too ineffective, or a combination of both.

14. The nature of filtering software and market are conducive to market failure because of the asymmetry of information between consumers and producers of the filtering software.

15. Because the market for filtering software is smaller than the markets for other kinds of software, software producers have a weaker incentive to improve the quality of filtering software products. This market failure is unlikely to be rectified.

16. Other potential alternatives to COPA are unlikely to be as effective in protecting minors from exposure to sexually explicit material on the World Wide Web. The creation of separate top-level domains for adult material, or for material designated as child-friendly, will not prevent minors from being exposed to sexually explicit material on the World Wide Web.

17. Voluntary efforts by parents to monitor their children's internet usage, or to educate their children about sexually explicit material on the World Wide Web, will not prevent minors from being exposed to such material.

18. An increase in obscenity prosecutions will not prevent minors from being exposed to sexually explicit material on the World Wide Web, because the scope of that material is broader than that of material that falls within the definition of obscenity.

19. COPA will be effective in protecting minors from exposure to sexually explicit material on the World Wide Web. The statute ensures that only adults will have access to harmful-to-minors material on the World Wide Web.

20. Website operators can easily comply with COPA. The placement of harmful-to-minors material behind a credit card screen is a valid affirmative defense under the statute. Credit cards are widely used on the World Wide Web, their use on the Web is easy to implement, and their use would ensure that only adults would have access to material behind the credit card screen. Online purchases made by those few children that have access to payment cards can easily and effectively be supervised by their parents.

21. Other technologies exist that will allow website operators to ensure that only adults would have access to harmful-to-minors material on their websites. For example, technology exists to permit website operators to process "micro-payments," and that technology can be used to ensure that the viewer of the website is an adult.

22. In addition, there are effective age verification services that are available for a website operator to use to ensure that only adults have access to his or her website, or to portions of his or her website.

23. The implementation of COPA will not have a significant negative impact on the development of commercial websites. The Internet is a stable, established business communications tool, and the implementation of COPA will not require the creation of new business models.

24. The implementation of COPA would not have a significant negative impact on viewers of websites. Consumers are willing to use credit cards on the World Wide Web, and are otherwise willing to share information in the course of viewing websites.

25. COPA would be effective in protecting minors from exposure to sexually explicit material on the World Wide Web, whether that material is produced in the United States or in other countries. A significant portion of that material is found on websites hosted in the United States. In any event, COPA can be enforced, either through prosecutions or through the enforcement of terms in payment agreements, against foreign producers of sexually explicit material who make that material available to minors in the United States over the World Wide Web.

II. PARTIES/STATUTORY BACKGROUND/PLAINTIFFS' FEAR OF PROSECUTION

A. Parties

26. Plaintiffs are either website operators, none of whom have anything to do with the commercial display and distribution of pornography on the Web, or associations suing on behalf of members who operate websites.

27. Plaintiff Addazi, Inc. d/b/a Condomania ("Condomania") alleges that it is "a leading online seller of condoms and distributor of safer-sex related materials." Am. Compl. at 12 ¶ 4. Condomania displays photographs of condoms, a product recommendation guide, and a safer sex manual. *Id.* at 32 ¶ 11. Condomania alleges that the Centers for Disease Control refers individuals to its website to answer questions, and Condomania "believes that the information it provides may prevent sexually transmitted disease and unwanted pregnancy among older minors and adults." *Id.* at 32-33 ¶¶ 13, 14. Condomania refers to the information it provides as "important information about sexuality and safer sex." The Condomania website states that

> At Condomania, we believe that the best way for the public to make educated choices about safer-sex products is through access to accurate, non-judgmental information. Our focus on education enables customers to feel comfortable asking questions and sharing ideas. We provide training to insure that the employees offer a supportive and friendly sounding board for customers' concerns. Condomania's vision is crucial to the prevention of unwanted pregnancies and sexually transmitted diseases, including HIV and AIDS.

28. Ms. Rearick's Scarlet Letters is "the Web's first artistic and educational site with a focus on women's sexuality. . . . Scarlet Letters publishes fiction, nonfiction, poetry, essays, commentary, visual art, and other material aimed at educating and entertaining its users." Am. Compl. at 34 ¶ 2. The Scarlet Letters website states that its "goal is to help eradicate sexual taboo, bias and stigma through creative expression and education."

29. Plaintiff Nerve.com "is an online magazine dedicated to a frank exploration of sex and sexuality. Nerve publishes content in a variety of formats, including but not limited to prose and poetry, photography, interviews, and reviews." Am. Compl. at 41 ¶ 23. Nerve does not allege that it exhibits material that is harmful to minors. It states that it "believes that sex as a topic has a distinctly political dimension," and much of the material on its site contains explicit and indirect political analysis.

30. "Nerve has won multiple awards for both its prose and photography." *Id.* The founder of Nerve testified that, while some may find Nerve's content titillating, "titillation tends not to be the primary objective of any of our content whether it's photography or writing. . . . There's little doubt in my mind that . . . our readers definitely see our content as being, you know, very smart, . . . serious, award-winning content." Deposition of Rufus Griscom at 20. Nerve was one of five finalists for the National Magazine Award for General Excellence Online in 2005, along with Atlantic Monthly, Consumer Reports, Business Weekly and Style.com. *Id.* at 79.

31. Plaintiff ACLU also sues on behalf of "a broad spectrum of members who use the Web to access material. Many ACLU members are minors, including both high school and college students, who will be directly affected by this Act." Am. Compl. at 26-27 ¶ 9. ACLU has not identified which websites ACLU members seek to access or how COPA would interfere with their specific intent to access such websites during discovery in this case.

32. Plaintiff American Booksellers Foundation for Free Expression is suing on behalf of its "bookseller members from coast to coast, many of whom sell materials that contain nudity or descriptions of the nude human body, and which deal frankly with the subject of human sexuality," and that "some bookstores have their own Web pages that discuss the content of

books sold in stores." Am. Compl. at 29 ¶ 1. During discovery, ABFFE identified only one bookstore on whose behalf it sues, the Sisterhood Bookstore, and this bookstore no longer has a website.

B. Statutory Background

33. COPA was passed as part of the Omnibus Consolidated and Emergency Supplemental Appropriations Act, 1999, Pub. L. No. 105-277, div. C, §§ 1401-06, 112 Stat. 2681, 2681-736 to 2681-741 (Oct. 21, 1998). The Act, codified at 47 U.S.C. §§ 230 & 231 (1998), was signed into law on October 21, 1998, with an effective date of November 20, 1998. This Court's temporary restraining order and subsequent entry of a preliminary injunction prevented COPA from going into effect on that date. *See American Civil Liberties Union v. Reno*, 31 F. Supp. 2d 473 (E.D. Pa. 1999). For ease of reference, citations to COPA herein will refer to its codification at 47 U.S.C. § 231.

C. Harmful to Minors Material on the Web

34. The federal government has a compelling interest in protecting minors from exposure to sexually explicit content on the World Wide Web.

35. A judge or jury is unlikely to find beyond a reasonable doubt that the web pages submitted by plaintiffs from Playboy.com are harmful to minors. Although one web page identified by plaintiffs from Playboy.com contains one photograph depicting female breasts, the majority of the pictures do not contain any nudity, and there is no depiction of sexual activity or full frontal nudity. The photographs from Playboy.com do not explicitly depict sexual acts or graphically focus on the genitals. (Def.'s 2d Supp. Response to Pls.' Contention Interrog. No. 15 (Sep. 27, 2006))

36. The web pages from Playboy.com are unlikely to be deemed to rise to the level of obscenity. (Def.'s 2d Supp. Response to Pls.' Contention Interrog. No. 16 (Sep. 27, 2006)).

37. Web pages submitted by plaintiffs from Penthouse.com contain lewd depictions of full-frontal nudity in its free content area, including a photograph of a woman exposing her labia and clitoris and a photograph of a woman turned to her side, spreading her buttocks, and revealing her vagina and anus. As a result, the web pages from Penthouse.com are likely designed to appeal to, or designed to pander to, the prurient interest and will likely be found to be patently offensive with respect to minors. These web pages are not saved from coverage by COPA because a court or jury likely would find that they do not have serious literary, artistic, political, or scientific value for minors. (Def.'s 2d Supp. Response to Pls.' Contention Interrog. No. 15 (Sep. 27, 2006))

38. Even the most graphic photographs submitted by plaintiffs from Penthouse.com—depictions of full female nudity—do not rise to the level of obscenity. Although this material may satisfy COPA's definition of "patently offensive" with respect to minors (*e.g.*, there is a graphic and lewd focus on the genitals), it is unlikely to be deemed patently offensive under the *Miller* test with respect to adults. (Def.'s 2d Supp. Response to Pls.' Contention Interrog. No. 16 (Sep. 27, 2006))

D. Plaintiffs' Fear of Prosecution

39. None of the plaintiffs is a commercial purveyor of what is commonly termed "pornography."

40. No plaintiff has demonstrated that his or her business, or any part thereof, is devoted to making harmful-to-minors communications for profit.

41. No website plaintiff has demonstrated that it intends to make harmful-to-minors communications for profit as a regular course of its business.

42. Plaintiffs' proffered expert, Henry Reichman, concluded that he "encountered nothing that could be deemed 'obscene' under my understanding of current legal standards or 'harmful to minors' under any reasonable definition of those words." (Reichman Report at 15)

43. Plaintiffs have had ample opportunity during discovery to offer objective facts and concrete examples to substantiate their fear of prosecution. Instead of providing Defendant with copies of web pages upon which they feared prosecution, Plaintiffs referred Defendant to their responses to Defendant's Interrogatory, in which he asked for representative samples about which Plaintiffs fear prosecution. (Pls.' Resp. to Def.'s Request for Docs. No. 13-15 [Attached as Ex. 3 to Def.'s Mot. to Dismiss)

44. A court or jury is unlikely to find beyond a reasonable doubt that any of the web pages submitted by plaintiffs violate COPA. None of the web pages are "designed to appeal to . . . the prurient interest," contain material that is "lewd" and "patently offensive with respect to minors," or otherwise "lack[] serious literary, artistic, political, or scientific value for minors." The Plaintiffs' websites contain, *inter alia*, scientific sexual education information, literary content, artistic content, and political content. For example, Sexual Health Network, Scarleteen, and Condomania provide valuable scientific information regarding sexual education. Other websites, such as Femmerotic and Nerve, show photographs with artistic value. Still others, such as Scarlet Letters, Salon, and Wildcat International evidence serious literary value for minors. (Def.'s 2d Supp. Response to Pls.' Contention Interrog. No. 11 (Sep. 27, 2006))

45. A court or jury is unlikely to find beyond a reasonable doubt that the specific web pages referenced above violate COPA because they are not designed to appeal to, or designed to

pander to, the prurient interest of 16 or 17 year-olds. For example, Sexual Health Network posts a response to a question about how to deal with a child who is caught having sexual relations with a dog. This web page, although dealing with a sexual theme, is not designed to appeal to the prurient interest. (Def.'s 2d Supp. Response to Pls.' Contention Interrog. No. 12 (Sep. 27, 2006))

46. To the extent plaintiffs have identified Web-based chat, e-mail, bulletin board, or discussion group areas on their Web sites, they have not alleged that they have knowledge of the information placed in these areas by users of their sites, so as to subject them to liability under COPA, 47 U.S.C. § 231(a)(7).

47. To the extent plaintiffs have identified Web-based chat, e-mail, bulletin board, or discussion group areas on their Web sites, they have not alleged that they actively take part in supervising or monitoring or filtering (*i.e.*, selecting or altering) information placed in these areas by users of their sites, so as to subject them to liability under COPA. 47 U.S.C. § 231(b)(4).

48. At least some of the plaintiffs have self-described policies, including advertising policies, that place content restrictions on what can be displayed on their sites, and plaintiffs intend to comply with those policies.

49. ACLU Member Lawrence Ferlinghetti stated that "[e]xamples of material that might be deemed 'harmful to minors' by some community in the United States include:

> 1) The City Lights Books website has a section with a history of the 'Howl' obscenity trial and photographs from the trial, located at http://www.citylights.com/His/CLhowl.html;
>
> 2) ACLU Member's work, which is available on a variety of poetry sites on the web, including the City Lights Books web site.

Pls.'s Resp. to Def.'s Interrog. No. 13. The only web page specifically identified by Mr. Ferlingehetti is a web page providing information about this history of Allen Ginsberg's poem

"Howl," and which is devoid of any sexual content. Mr. Ferlinghetti did not identify the ACLU Member poetry he believes is harmful to minors during the discovery period.

50. ACLU Member Patricia Nell Warren listed six examples of material that "might be deemed harmful to minors by some community." Pls.'s Resp. to Def.'s Interrog. No. 13. The first example is a commentary on the death of Matthew Shepard, a college student who was beaten to death in 1998 in what was widely perceived to be a hate crime based on sexual orientation. *See id.*

51. The other five web pages for which Ms. Warren fears prosecution are excerpts from five of her novels. Each of the books excerpted on Ms. Warren's website are sold on mainstream outlets such as Amazon.com.

52. The representative sample of material upon which Condomania fears prosecution are: (1) a page discussing safer sex; (2) product reviews of condoms; (3) a "condom wizard" page for a cartoon-led interactive shopping experience; (4) a page selling gifts and novelties; and (5) a blog entitled "Condoms, Sex, and Desire" that discusses topics such as National HIV Testing Day, comments on the products sold on Condomania, and Internet Sexuality Information Services. Pl.'s Resp. to Def.'s Interrog. No. 13. The pages for which Condomania fears prosecution contain factual information for education and sales of safer-sex products and contain no nudity whatsoever. *Id.*

53. Plaintiffs' proffered expert, Henry Reichman, concludes that material on Condomania provides sex education and "post-pubescent teenagers can . . . find useful information there." Reichman Report at 16. He also concludes that the material on Condomania "is by no reasonable definition obscene or harmful to minors." *Id.*

54. Scarleteen is meant for an audience of minors and provides, as the Amended Complaint describes, "teen-oriented" content. Am. Compl. at 35 ¶ 3. Ms. Rearick stated in her deposition that the content on the Scarleteen website is driven by the teenage viewers of the website. Deposition of Heather C. Rearick at 84, 86. The pages offer health, scientific, and political information specifically geared toward teenagers. In addition, it does not contain any photographs of sexual acts. It also has serious scientific value for minors. In fact, the online encyclopedia Wikipedia references Scarleteen for anatomy articles. *See id.* at 88-89.

55. Ms. Rearick identified several pages in her deposition about which she feared prosecution under COPA. These pages are: an article about a 15-year old's experience with being a gay teenager, instructions for putting on a condom, and the Scarleteen message boards. Rearick Dep. at 71, 81, 244-45. The information contained in these pages is age-appropriate for older minors, which is the goal of the Scarleteen website. Rearick Dep. at 46-48; 143-44.

56. Scarleteen maintains a policy for message board postings, and if something inappropriate is posted, Ms. Rearick edits it. *See* Rearick Dep. at 28:110-17.

57. For Ms. Rearick's website Scarlet Letters, she specifically identified only the front pages of each section of her website, including visual art and photography, prose and poetry, nonfiction, and forums, as a representative sample of pages about which she feared prosecution. While Ms. Rearick stated, as a general matter, that she feared prosecution based on the forum for Scarlet Letters, she admitted at her deposition that "I haven't looked at the message boards in so long that I couldn't begin to tell you what they are." Rearick Dep. at 171.

58. "Femmerotic is Heather Corinna's personal Web site for showcasing her photographic and textual work and providing an 'open and intimate look at her life as an artist and activist.'" Am. Compl. at 35 ¶ 4. In her interrogatory responses, Ms. Rearick did not

identify any specific web pages as a representative sample about which she fears prosecution. She stated that the Gallery (Photography) section of the website contains "numerous nude photographs of Plaintiff and others," that the Journal section of the website contains "explicit discussions of sexuality," and that the FAQ section of the website "contains frank discussions of sexuality." The only FAQ page on the website relates to her journal, which contains no sexually explicit material.

59. Femmerotic has a subscription-only area, which users can access with a credit card payment. Rearick Dep. at 246. In her deposition, Ms. Rearick alleged a fear of prosecution for the subscription material, which she described as "much more explicit" than the publicly available portions of the website. *Id.*

60. Mr. Boushka alleges to fear prosecution for the other content on his current website, which consist of four of his screenplays. He alleges that these screenplays contain "frank portrayals of sexual desire between younger and older men," with one of those screenplays containing descriptions of nudity. None of the screenplays contain explicit sexual content.

61. The two videos currently on the Web – Radical Sex Workshops and TLC2 – are short documentaries involving the Tarheel Leather Club. They address the social support system of "leather clubs" and interview several members of the club. They also discuss the impact of AIDS on the leather community, safe sex, and one video has footage of workshops in which instructors discuss sexual techniques and safety. There is no nudity in either video.

62. Free Speech Media's community page is a forum for political discussion and does not have any material with sexual content.

63. The two examples that Nerve lists in the Amended Complaint about which it fears prosecution (the Courting of Anatomy and Mystery Tour), are available only to premium members, which are not available without the input of credit card information.

64. Nerve's founder testified that he believes Nerve has serious value for older minors. *Id.* at 133. Nerve has never taken any steps to associate itself with pornographic websites, *id.* at 57-58, and it has a policy not to accept explicit adult advertising. *Id.* at 16-17.

65. The Urban Dictionary Web site encourages users, including minors, to understand, participate, and take ownership of the English language and its constantly evolving definitions." Am. Compl. at 43 ¶ 4. The website is "user-generated" and Mr. Peckham states that he "has little ability to ensure that users comply with a 'harmful to minors' standard." Am. Compl. at 43-44 ¶ 4. The Urban Dictionary website does not have a "pre-approval process" for submissions. *Id.*

66. PGN's classified advertisements (including the adult classified ads) are advertisements of an informational nature.

67. PGN is a newspaper like many others throughout the country that cover serious issues and contain, as a small part of its publication, classified advertising. Plaintiffs' proffered expert, Henry Reichman, asserts that PGN "is not an explicitly sexual site by any reasonable definition." Reichman Report at 25.

68. Powell's identifies reviews of the books "Joy of Gay Sex Fully Revised 3rd Edition" and "The Many Joys of Sex Toys: The Ultimate How-To Handbook for Couples and Singles" as material upon which it fears prosecution. *See id.* In discovery, Powell's listed web pages describing eight books as a representative sample about which it feared prosecution. All of the books advertised are literature that would be sold in general interest bookstores. The

reviews and excerpts contained on Powell's website have literary, artistic, political, or scientific value for minors, as they all describe the books in a straightforward and informative manner.

69. Salon has stated that it does not fear prosecution under state harmful-to-minors laws because it does not believe that they "would apply to the kind of content that we post on Salon." Walsh Dep. at 112-13. Nevertheless, Salon alleges a fear of prosecution under COPA.

70. In the Amended Complaint, Salon proffered three articles it believes could be considered to be "harmful to minors" in some communities. *See* Am. Compl. at 49-50 ¶ 6. One article involves "the rhetorical implications of the word 'pussy'" and the author's "belief that it is a word in need of reclamation." *Id.* Salon printed the article because it thought the article contained a provocative argument about the misogynistic use of the term, and Salon views the article as a serious article. Walsh Dep. at 99-100. The second article is a serious article about pornography, which Salon published because it thought the author was "a good writer with a unique voice on these topics. We think her history as a feminist and her evolution in the way she thinks about sexuality and even what's considered pornography is provocative and that she has interesting and unusual insights." *Id.* at 102. Salon did not publish this article to appeal to the prurient interest. *Id.* at 102-03. The third article mentioned in the Amended Complaint is an interview with an author who had written a book about anal sex. Salon published the article because the book "was a widely-reviewed book by a relatively serious writer and was attracting all kinds of interest, and our staff writer wanted to explore the contradictions of this woman who considers herself a feminist writing a book called 'The Surrender,' and talking about how important it was to be dominated in this particular way by a man." *Id.* at 105. Salon had a serious intent in printing the article, and did not do so to appeal to the prurient interest. *Id.* at

105-06. According to Salon's editor-in-chief, none of the articles listed in the Amended Complaint were "beyond the mainstream." *Id.* at 106.

71. In discovery, Salon did not provide any additional representative examples about which it fears prosecution. Rather, it generally stated that it fears prosecution for "articles discussing, among other things, various forms of sexual contact and activity, human genitalia, and human sexuality generally" in six topic areas of the website (sex, sexuality, homosexuality, gay, lesbians, and oral sex). In addition, Salon states that it has a dialogue section where web users can directly post comments "on a diverse category of topics." *Id.* Salon fears prosecution because it contains articles dealing with sex and sexuality. The editor-in-chief of Salon testified that she did not consider any portion of the Salon website to be pornographic. Walsh Dep. at 39.

72. Salon also identified sections of its website where users directly post comments as containing material about which it fears prosecution. The areas of Salon where users directly post material are: The Well, Table Talk, and Salon Blogs. The Well is a separate website, and requires a paid subscription. *See* Walsh Dep. at 52; *see also* http://www.well.com/. Salon states that bloggers have "complete autonomy to put their words on the site. and that Salon does "not really" monitor the threads on the Table Talk section, and that they have a half-time person to moderate the tens of thousands of posts." Walsh Dep. at 40, 45-46.

73. Salon has not produced any evidence that these sections where contirbutors post matertial contain any sexually explicit material. The editor-in-chief of Salon testified that the blog section of Salon does not contain sexually explicit photos. Walsh Dep. at 43.

74. Dr. Tepper testified that his website, Sexual Health Network provides social value to minors. Deposition of Mitchell Tepper at 103. The material upon which Sexual Health Network alleges a fear of prosecution renders advice in a scientific manner. Dr. Tepper has

never received a complaint from anyone that the material on Sexual Health Network is harmful to minors. Tepper Dep. at 96.

75. Dr. Tepper's fear of prosecution rests on several factors: restrictions on what can be taught to minors for entities receiving federal funds; professional harm college professors have suffered for giving sexuality education; and the federal government's belief about appropriate sexual education and its policies about what should be taught. *See* Tepper Dep. at 134-40. Plaintiffs' proffered expert, Henry Reichman, has concluded that the material posted on Sexual Health Network is educational and "is by no reasonable definition obscene or harmful to minors." Reichman Report at 16.

III. EXPERT QUALIFICATIONS

76. Philip Stark is qualified to testify as an expert with regard to the application of statistical techniques to the Internet. In particular, he is qualified to testify as an expert with regard to his application of statistical techniques to a study that he and Paul Mewett performed of the prevalence of sexually explicit web pages on the World Wide Web and of the effectiveness of filtering software in blocking access to such pages. (Stark Report)

77. Philip Stark is a member of the American Geophysical Union, the Bernoulli Society for Mathematical Statistics and Probability, the Center for Astrostatistics, the Center for Data Analysis Technology and Applications, the Global Oscillation Network Group, the Institute of Physics, the Institute of Mathematical Statistics, the National Partnership for Advanced Computational Infrastructure, the Royal Astronomical Society, the Solar and Heliospheric Observatory Solar Oscillations Investigation, the Space Sciences Laboratory, and the Theoretical Astrophysics Center. (Stark Report)

78. Paul Mewett is qualified to testify as an expert with regard to technical aspects of the operations of computers and of the Internet and the World Wide Web. In particular, he is qualified to testify as an expert with regard to a study that he and Philip Stark performed of the prevalence of sexually explicit web pages on the World Wide Web and of the effectiveness of filtering software in blocking access to such pages. (Mewett Report)

79. As the head of the Internet Intelligence Unit, Paul Mewett uses his skills and knowledge relating to mining the Internet and other electronic media to support the investigations of the Forensic Investigations Practice and the Computer Forensics Practice. (Mewett Report)

80. Over the last four years, Paul Mewett has worked with law enforcement in North America and in the United Kingdom, as well as the National Center for Missing and Exploited Children, where he has managed the technical challenges relating to tracking and identifying child pornography on the Internet. (Mewett Report)

81. Paul Mewett has also run programs to track credit card fraud and identity theft which takes place in the Deep Web. These programs require Mr. Mewett to apply his comprehensive knowledge of the Internet, its architecture, and the technical innovations that have enabled the Internet's rapid expansion. (Mewett Report)

82. Paul Mewett has performed analysis for a number of clients that involved gathering of data sets and drawing conclusions from the data that was collected. As one example, he recently performed a study for a mobile telecommunications client that involved identifying locations on the Internet that were sharing intellectual property, and that also involved analyzing those Websites to determine if the operators of those Websites could be located. (Mewett Dep. at 233-34.)

83. Before joining CRA International, Paul Mewett founded and took public a company that focused on the retrieval of information from the Internet for large companies. He was instrumental in the design and development of the spider technology, as well as the business strategy, that made the company a success. That spider technology was created specifically to be able to "crawl" around the Surface Web and to identify information specific to a company's name or brand. Mr. Mewett's clients for this technology included a number of global banks, a major German automotive company, a pharmaceutical company, and a major global health care company. (Mewett Report)

84. Paul Mewett has also held the post of Chief Technical Officer for another company, ASP Solutions Ltd., in the field of Internet Intelligence Solutions. The company used "best of breed" and in-house tools to identify and deliver business intelliegence from the Surface Web and the Deep Web for major branded clients. (Mewett Report)

85. Prior to joining CapAnalysis in 2003, Dr. Eisenach served for 10 years as President of the Progress & Freedom Foundation, a research organization that studies the Internet and its implications for public policy. While in that position, he authored or co-authored more than two dozen research papers and submissions to regulatory agencies on the Internet and communications issues, including an annual volume called the Digital Economy Fact Book, which is a compilation of economic data relating to the Internet, communications technologies and software. Dr. Eisenach's opinions on the effectiveness of filtering software are based on his experience and on general assumptions made in microeconomic research of consumer behavior regarding ICF products, as well as consumer survey research. Eisenach Dep. at 53:9-54:21, 55:13-19.

86. Stephen Neale is qualified to testify as an expert regarding issues in the field of linguistics relating to the efficacy of internet content filtering software.

87. His area of expertise is what is usually called the philosophy of language, which includes the study of syntax, semantics, logical analysis, formal systems, computability theory, context, translation and interpretation, all of which he has worked on extensively.

88. Mr. Clark has significant experience in reading research results from both his corporate experience and his consulting experience, including working with research departments in designing studies to meet business needs, so that the data from the study is projectable and usable for business purposes. He has had a great deal of influence on whether survey research is conducted over the phone, in person, or in focus groups in both quantitative and qualitative research, and has played a significant role in determining the sample sizes of the survey research. Industry research and consumer research is at the core of Mr. Clark's ability to do his job. His firm is constantly assembling proprietary data on rates of fraudulent and/or unauthorized uses of payment cards and rates of adoption and/or use of payment cards across various segments of the population in different types of sales transactions. Clark Dep. at 7:20 – 8:22; 15:14-17.

89. Mr. Clark has experience in marketing prepaid cards to the youth market from a project he did and is doing for First Financial Bank, which focuses on the youth market. Clark Dep. 99:8-13.

90. Mr. Clark is an expert in payment cards, including, among other things, what payment cards are used for on the Internet by consumers and merchants, how they work, the adoption rates, fraud rates, and the amount of payments per transaction. Clark Dep. at 7:11-13, 9:19-25.

91. Mr. Clark is qualified to opine on the effectiveness of COPA's credit card and debit account affirmative defenses.

92. Dr. Smith is an expert in (1) Internet research and methodology; (2) advanced computer applications for Internet survey research and analysis; (3) cross-cultural research; (4) consumer behavior; and (5) Internet business models. He has co-authored a textbook on the fundamentals of market research, and has authored or co-authored twelve books or monographs and more than 60 articles or papers, including a book on Internet marketing. He has worked as a research consultant for IBM, Microsoft, and Yahoo!

93. Dr. Smith is qualified to testify about the effect COPA would have on the Web.

94. Dr. Smith is the Founder and Director of Qualtrics, Inc., SurveyZ.com, and SurveyPro.com. These online Applications offer the most advanced survey research, database, and analysis tools available and are used by companies like the U.S. Army, The Conference Board, Celebrity Cruises, Intel, Kodak, Micron, Yahoo!, Microsoft, Travelocity, ATI, Sabre Holdings, Royal Caribbean, and Motorola.

95. Dr. Smith has served on the editorial board of Health Marketing Quarterly, Journal of Health Care Marketing and has reviewed for Journal of Marketing Research, and the Journal of the Academy of Marketing Science. He is the past president of the Association for Health Care Research.

96. Dr. Smith has instructed executive courses in research methodology for IBM Corporation and the American Marketing Association Professional Division and has been an active research consultant for the following companies: IBM, Microsoft, Yahoo!, ATI, Iomega, Bell South, Caterpillar, Johnson and Johnson, Miles Labs, Nissan, Novell, Pioneer-Hi-bred Seed Company, Quaker, Sarah Lee, Staples, Simplot, and the U.S. Army.

97. Dr. Smith currently teaches "Marketing Research," "Measurement and Analysis," and "Field Studies" courses in the undergraduate and MBA programs at BYU. My earned degrees are from Brigham Young University (B.S. Business, 1971), Michigan State (MBA, 1973), and Pennsylvania State University (Ph.D., 1979). Dr. Smith wrote his dissertation on segmenting retail shoppers.

98. Each of defendant's principal expert reports produced by Professor Stark, Mr. Mewett, Professor Neale, Dr. Eisenach, Mr. Clark, and Dr. Smith is authentic and admissible as evidence in this case.

99. Each of defendant's expert rebuttal reports produced by Mr. Mewett, Dr. Eisenach, and Mr. Clark is authentic and admissible as evidence in this case.

IV. THE STATUS QUO

A. The World Wide Web

100. The primary method of remote information retrieval over the Internet today is the World Wide Web ("WWW" or simply the "Web"). The Web is a global information space operating over the Internet, which people can read from and write to via a variety of different Internet-connected devices, including for example, computers, Personal Digital Assistants ("PDAs"), and cellular phones. Mewett Report ¶ 8.

101. The Web is a service that operates over the Internet. The Web is the complete set of documents residing on all Internet servers that use the Hypertext Transfer Protocol ("HTTP"), which is the protocol specifying how hypertext will be moved around the Web. Mewett Report ¶ 9.

102. The World Wide Web combines four basic components:

a. Hypertext, that is the ability, in a computer environment, to move from one part of a document to another, or from one document to another, through internal connections among these documents (called "hyperlinks" or "links");

b. Resource Identifiers, that is the ability, on a computer network, to locate a particular resource (computer, document or other resource) on the network through a unique identifier;

c. The Client-server model of computing, in which client software or a client computer makes requests of server software or a server computer that provides the client with resources or services, such as data or files; and

d. Markup language, in which characters or codes embedded in text indicate to a computer how to print or display the text, *e.g.* as in italics or bold type or font.

Mewett Report ¶ 10.

103. When a viewer wants to access a Web page or other "resource" on the World Wide Web, he or she normally begins either by typing the Uniform Resource Locator ("URL") of the page into his or her Web browser, or by following a hypertext link to that page or resource. When the viewer does so, the server-name part of the URL is "resolved," or translated, into an Internet Protocol ("IP") address by the global, distributed Internet database known as the Domain Name System ("DNS"). This database stores all the registered domain names and associated IP addresses. When a user types in a domain name, the system looks it up and then uses for all remaining references the associated IP address that was found in the database. A Domain Name is the name that identifies one or more IP addresses on the Internet. The system allows people to refer to locations on the Internet by names, while the computers on the Internet can communicate by referring to each other as numbers. The IP address is the numerical identifier for a computer or device on the Transmission Control Protocol/Internet Protocol ("TCP/IP") network. Mewett Report ¶ 12.

104. Some Web sites, in addition to displaying the page requested by the user, will also display content using "pop-up screens." These pop-ups open without prompting by the user.

Pop-ups are most commonly used on commercial sites for advertisements, which may or may not be topically related to the content of the original Web site.

105. Some Web sites will automatically open new windows that a user did not affirmatively take steps to access, or will re-direct the user to a different site altogether.

106. The result of a Web search is usually a list of URLs with short explanatory summaries. Search engines do not search the Web; instead, they search regularly updated indexes to operate quickly and efficiently. Mewett Report ¶ 14.

107. Search engines obtain their Web page listings in two ways. Web site operators may submit their own Web pages to the search engines, or the search engines may "crawl" or "spider" documents by following one hypertext link to another. The latter process returns the bulk of the Web pages and associated URL listings contained in search engine databases. Crawlers work by tracking and recording hypertext links in the Web pages that they index while crawling. Mewett Report ¶ 19. A copy of each Web page visited is then stored on the search engine servers. These servers are generally located in server farms, and the major search engines may operate many thousands of these servers. When a user enters a query on a search engine via their browser, that query is sent to the databases on these servers. Mewett Report ¶ 20.

108. Search engines such as Google, MSN or Yahoo! Search, and directories such as Yahoo! Directory, give access to only a small part (less than 10 percent) of the Web. This portion of the Web is often referred to as the Surface Web or the "Accessible" Web. The technology used by these conventional search engines does not provide access into a vast area of the Web called the Deep Web, which is much larger than the Surface Web. Mewett Report ¶ 16.

109. The Deep Web is composed of Web documents that are poorly indexed or not indexed at all by the broad-based conventional search engines. Mewett Report ¶ 21. Pages on

the Deep Web comprise a variety of materials, including dynamic content, databases, documents omitted because they are too large, pages protected by the author, and pages with restricted access. Mewett Report ¶ 23.

110. Most users of the Internet who start their typical surfing journey using a search engine will initially view the Surface Web. However, once links start to be clicked and the journey progresses, the likelihood of staying in the Surface Web diminishes. Mewett Report ¶ 24.

111. It is becoming more likely that users of the Internet will be steered to content in the Deep Web, for several reasons. Web content providers increasingly use dynamic content in their Web sites. In addition, some Web content providers use URL redirection to steer viewers from the URL that they intended to access to a different URL. Redirected content frequently is found in the much larger, less structured Deep Web. Mewett Report ¶ 25.

112. It is not possible to determine precisely the number of Web pages in either the Surface Web or the Deep Web. The Surface Web has been reasonably estimated to be anywhere between 25 billion and 64 billion pages in size as of 2005, with an estimated 50 million pages being modified or added every day. The Deep Web has been estimated to be over 500 times larger than the Surface Web. Mewett Report ¶¶ 17, 31.

B. Sexually Explicit Content on the Web

113. Paul Mewett of CRA International, Inc., and Dr. Philip B. Stark, Ph.D., performed a study of sexually explicit material on the World Wide Web on behalf of the defendant. For the purpose of this study, several samples of URLs were drawn. First, a random sample was drawn of the URLs available in the index maintained by Google Inc. for its search engine. Second, a random sample was drawn of the URLs available in the index maintained by the Microsoft

Corporation for its MSN search engine. Third, a random sample was drawn of actual queries entered into the MSN, Yahoo!, and AOL search engines, and the URLs returned by the search engines from the queries in that sample were studied. Fourth, a study was performed of URLs returned by search engines from the most popular queries, as recorded by Wordtracker. (Wordtracker is a service that collects queries from several search engine aggregators.)

114. Approximately 1.1 percent of the Web pages in both the Google and MSN indexes are sexually explicit. It is therefore reasonable to estimate that between 275 million and 704 million of the Web pages on the Surface Web are sexually explicit. (Stark Report ¶ 10; Mewett Report ¶¶ 31, 71)

115. In addition, sexually explicit Web pages are returned more frequently in response to search engine queries than are other searches. Approximately 1.7 percent of the URLs returned from the search engine query data set from MSN, Yahoo!, and AOL are sexually explicit. Approximately 6 percent of the queries in that data set return at least one sexually explicit Web page in response to the query. (Stark Report)

116. Sexually explicit Web pages are returned significantly more frequently in response to the most popular search engine queries. Approximately 14.1 percent of the URLs returned in response to the search engine query data set from Wordtracker are sexually explicit. Approximately 37.1 percent of the queries in that data set return at least one sexually explicit Web page in response to the query. (Stark Report)

117. Even seemingly innocent popular queries will return sexually explicit material. An examination of the data set from Wordtracker reveals that innocuous queries such as “Online Games” and “Oops” return sexually explicit material. Mewett Report ¶ 57.

118. Envisional, a company that operates a search facility for companies that can detect online misrepresentations of their brands, performed a study on children's toy brands. Its search of the 26 most popular children's characters, including Pokemon, My Little Pony, Toy Story and Furby, revealed several thousand links to pornographic sites. Thirty percent of these sites featured hard core sexually explicit material. The remainder of those linked sites contained nudity, obscene language or extreme violence. Mewett Report ¶ 57.

119. Of the sexually explicit Web pages in the Google index, approximately 44.2 percent are domestic, that is, are hosted in the United States. Of the sexually explicit Web pages in the MSN index, approximately 56.7 percent are domestic. Stark Report ¶ 10; Stark Rebuttal Report.

120. Domestic sexually explicit sites appear to be especially popular in comparison to foreign sexually explicit sites. Of the sexually explicit Web pages in the set of URLs returned from the sample set of search engine queries, approximately 88.4 percent are domestic. Similarly, of the sexually explicit Web pages in the set of URLs returned from the Wordtracker set of the most popular queries, approximately 87.4 percent are domestic. Stark Report.

121. The majority of sexually explicit websites are commercially driven. Zook Report at 3. The sexually explicit websites can be categorized into two groups – "feeder" websites, and membership websites or "pay sites." Zook Report at 4.

122. Membership sexually explicit websites use feeder websites as "bait" for the pay sites, and the feeder websites make their money by successfully guiding viewers to premium services on other websites. Zook Report at 4.

123. Affiliate fees from the membership websites are the primary source of revenue for feeder sexually explicit websites. Zook Deposition at 50.

124. Feeder adult websites offer pictures amidst a maze of banners and pop-up windows that direct visitors to membership websites. Zook Report at 4.

125. Because of large bandwidth requirements, companies specializing in the adult industry, rather than traditional hosting services, generally host adult websites. Because traffic to adult websites can build quickly, hosting is generally the most significant cost to websites. Zook Report at 5.

126. These hosting costs make the paid membership websites essential to the functioning of a commercial Internet adult industry. The more content that is downloaded from a website, the higher consumption of bandwidth. Without paid memberships, the Internet adult industry could not pay for the bandwidth that it consumes. Zook Report at 5.

127. According to an article published in 2003 by Matthew Zook, approximately 85 percent all adult membership websites are hosted in the United States. Zook Dep. at 63. 93.3 percent of all feeder adult websites are hosted in the United States. Zook Dep. at 64.

128. Membership adult websites would face some barriers in relocating outside of the United States, as it would be more difficult to process credit card fees, to generate new content, or to manage memberships. Zook Dep. at 54.

C. Children's Access to Commercial Pornography on the Web

129. The World Wide Web is widely accessible by minors. According to a recent study conducted on behalf of the U.S. Department of Education, approximately 59 percent of all students (from nursery school through the 12th grade) use the Internet. Twenty-three percent of students in nursery school use the Internet, as do 32 percent of students in kindergarten, 50 percent of students in the 1st through 5th grades, 70 percent of students in the 6th through 8th grades, and 79 percent of students in the 9th through 12th grades. Matthew DeBell and Chris

Chapman, Computer and Internet Use by Students in 2003: Statistical Analysis Report at 6 (Sept. 5, 2006).

130. In light of the widespread availability of the Internet, a parent cannot guarantee that his or her child will not have access to sexually explicit material, even if he or she were to take the drastic step of removing computers from the home. In addition to using the Internet in their own homes, 43 percent of all students use the Internet at school, 10 percent use the Internet at libraries, and nine percent use the Internet at other person's homes. (Id. at 25.)

131. Minors who can read and type are capable of conducting Web searches as easily as operating a television remote. While a four-year-old may not be as capable as a thirteen-year-old, given the right tools (*e.g.*, a mouse and browser software) each has the ability to "surf" the Web and will likely be exposed to harmful material. (H.R. Rep. No. 105-775, at 9-10.)

132. Many of the numerous adult sites on the World Wide Web openly allow children under the age of 17 to see hard-core and soft-core pornography pictures for free by simply clicking on any link to an adult pornography site's home Web page. (H.R. Rep. No. 105-775, at 10.)

133. Such pictures are listed under various types of banner or titles, including "Previews," "Teasers," "Guests," "Free Samples," "Free Pictures," which when clicked on will allow the visitor to see both images and text. (H.R. Rep. No. 105-775, at 10)

134. All of the types of free samples referred to above are photographs or short video clips or video outtakes of X-rated movies, including amateur and "home" movies.

135. Even if the drastic step of ridding the household of computers were taken, minors still will have access to harmful material from computers with Internet connections located in

schools, libraries, retail outlets, and other people's homes, as well as Internet access over cell phones, personal digital assistants, and other electronic media.

136. Ernie Allen is President and Chief Executive Officer of the National Center for Missing and Exploited Children ("NCMEC").

137. Established in 1984, NCMEC's mission is to help prevent child abduction and sexual exploitation; help find missing children and assist victims of child abduction and sexual exploitation, their families, and the professionals who serve them.

138. NCMEC is a resource for Congress, and does not lobby Congress.

139. NCMEC was not required by the Justice Department, Congress, or anyone else, to commission either the 1999 or 2005 Online Victimization of Youth study as a condition of receiving funding.

140. David Finkelhor, Ph.D., is the Director of the Crimes Against Children Research Center ("CCRC") at the University of New Hampshire.

141. In 1999, NCMEC commissioned the CCRC to conduct the first Online Victimization of Youth study ("*YISS-1*"), because there were not studies of the incidents of sexual solicitations, unwanted exposure to sexual material, and online harassment of youth ages 10-17 who use the Internet.

142. NCMEC sought to learn from the first Online Victimization of Youth study (1) what are the problems associated with Internet sexual solicitations, unwanted exposure to sexual material, and online harassment of minors ages 10-17, (2) how serious those problems are, and (3) who was most affected by those problems.

143. *YISS-1*, which was based on telephone interviews of a nationally representative sample of 1501 youths ages 10-17 who use the Internet regularly, and their parents and

guardians, found, *inter alia*, that one-third of parents and guardians of the youths had at the time of the interviews filtering or blocking software on the youths' computers at home. *YISS-1* at ix.

144. *YISS-1* found also that one-quarter of the interviewed youths had in the past year been exposed to unwanted sexual material while using the Internet at home. *YISS-1* at ix.

145. In 2005, NCMEC commissioned CCRC, under Dr. Finkelhor's oversight, to conduct the second Online Victimization of Youth study ("*YISS-2*") in order to measure changes since *YISS-1*. The results of *YISS-2* were released on August 9, 2006.

146. *YISS-2* is authentic and admissible.

147. In 2005, NCMEC commissioned the second Online Victimization of Youth study to measure changes since the first study, and the results were released on August 9, 2006.

148. The second study shows that, despite an increase in filter use, the rate of unwanted sexual material reaching 10-17 year-olds has risen. *YISS-2* at 1.

149. In carrying out the *YISS-2* survey, CCRC conducted telephone surveys of representative national samples of 1500 youth Internet users, ages 10 through 17. *YISS-2* at 4. Parents or guardians were interviewed first, for about 10 minutes, and with the consent of the parents or guardians, the youths were interviewed for about 30 minutes. *Id.* The interviews involved dozens, if not more than a hundred questions. The interviews were conducted from March to June 2005. *Id*.

150. The 2005 study noted that the increase in youths' exposure to unwanted sexual material occurred after the enactment of 18 U.S.C. § 2252B in 2003, which made it a criminal offense to use a misleading domain name on the Internet with the intent of deceiving a minor into viewing harmful sexual material. *Id*. at 8 n.8.

151. The 2005 study also reported a larger proportion of exposure incidents happened when youths were "surfing" the Web - 83 percent (*YISS-2)* compared to 71 percent (*YISS-1*). *Id*. at 9, 30. More than one-third of surfing exposure incidents happened when youths were doing online searches (40 percent), clicking on other links in other web sites led to 17 percent of exposures, misspelled web addresses led to 12 percent, and 14 percent were from pop-up ads. *Id*. at 30, 36. In *YISS-2*, 18 percent of youth with unwanted exposures while surfing online said they were brought to another sex site when they tried exiting the first site they were in. *Id*. at 32.

152. Pornography sites are sometimes "mousetrapped" or programmed to make them difficult to exit. Clicking an exit button takes viewers into another sexually explicit site instead of allowing them to leave. *Id*.

153. The 2005 survey addressed, *inter alia*, unwanted exposure of minors to sexually explicit material on the Web. *Id.*

154. With respect to the topic of unwanted exposure to sexual material, the 2005 survey focused, *inter alia*, on the level of Internet use both in terms of number of days online per week and the number of hours per day; the number of youth who had access at home, school and in other locations; the type of Internet access – dial-up or broad-band; marketing of sexual material via the Internet; and the efficacy of filters and spam blockers on computers in youths' homes and in other locations. *Id*. at 9-10.

155. The 2005 survey found, *inter alia*, that 47 percent of the parents and guardians with home Internet access had at the time of the interview software on the children's computer to filter sexually explicit images or web sites. *Id*. at 46.

156. The 2005 survey found, *inter alia*, that despite a reported increase in filtering, blocking, and monitoring software usage from 33 percent (in 2000) to 55 percent for all three

types of software (in 2005), the surveyed youths' exposure to unwanted sexual material rose from one-quarter to 34 percent during that time frame. *Id.* at 1.

157. The 2005 survey found, *inter alia*, that exposure incidents that were very or extremely upsetting to youths–distressing exposures--had increased from 6 percent in *YISS-1* to 9 percent in *YISS-2*. *Id*. at 9.

158. Based on the wide variety of search terms that led youth to unwanted sexual material as reported in *YISS-2*, apparently even innocent search terms may lead to material that is inappropriate for minors. *Id*. at 32.

159. One of the recommendations from *YISS-2* is the need to evaluate and improve filtering, blocking, and monitoring software solutions, as there is an apparent large gap between what consumers want and need and what they end up using. *Id*. at 64.

160. A 2002 report found that 25 percent of minors surveyed between the ages of 10 and 17 who regularly use the Internet inadvertently viewed pornography in the prior year. That number jumps to 70 percent when focused on minors between the ages of 15 and 17. National Research Council ("NRC"), YOUTH, PORNOGRAPHY, AND THE INTERNET 132-33 (Dick Thornburgh & Herbert S. Lin eds., 2002).

161. According to the NRC report, "it is probably not feasible [for parents] to provide constant supervision of [a] child's Internet access, especially as [the] child gets older." (NRC Report at 223)

162. The NRC report concludes that, while parental supervision and education may be useful in part to counter the problem of minors' exposure to sexual materials on the Internet, "the expectations for such education and socialization should not be unrealistic." (NRC Report at 371)

D. Effectiveness of Internet Content Filters

163. Corporate and educational Internet content filtering products are marketed for and designed to be implemented in a different environment than residential Internet content filtering products. Eisenach Rebuttal Report ¶¶ 26, 27.

164. Residential PC-based Internet content filtering programs generally work by installing themselves between the application layer (such as the browser) and the protocol layer (the mechanism for transporting data across computer networks). The software then acts as a conduit between the browser and the Web server, where it intercepts outbound requests and inbound data in order to filter them. Mewett Report ¶ 33; Neale Report, ¶ 4.3.

165. Internet content filters use two main approaches, normally in tandem. The first approach uses a "black list" of known Web sites, areas within Web sites, or specific Web pages. Outbound requests are checked against this list, and the software attempts to block the requested material if it matches the list. Mewett Report ¶ 34.

166. The second approach involves "dynamic filtering," *i.e.*, the checking of inbound data against keywords and/or phrases in an attempt to establish if that data contains content that contravenes the filtering rules. If it does, then the software attempts to block the data. Internet content filtering companies use a variety of proprietary algorithms to achieve this process. In essence, however, they all attempt to achieve the same result, that is, determining whether there are sufficient words, or a particular usage of words, to justify blocking the page. Text filtering at this stage can take place in either the URL itself (*i.e.*, does a particular term exist within the URL), within the text on the page or source code associated with the page, or finally in the links on the page to other pages within the site or other sites. Mewett Report ¶ 34; Neale Report, ¶ 3.3.1 - 5.

167. The task of keeping an up-to-date "black list" is mammoth. After entries have been initially categorized, they need to be regularly rechecked to confirm that the site has not changed its content, and therefore is in need of recategorization. As new domains continue to become available, the number of possible domains that must be analyzed for possible inclusion in a "black list" grows too. This increase forces a major dependency on the real-time analysis technology being employed to evaluate the page. For example, a survey in April 2006 by the company Netcraft identified in excess of 80 million domains in use world wide. Mewett Report ¶ 35.

168. The sheer size of the Web means only a very small (and shrinking) proportion of existing Web pages and Web sites can be classified by hand (*i.e.*, on the basis of subjective decisions made by human reviewers); so the overall effectiveness of a filter will always be a function of the performance of its automated classification software. (Mewett Testimony; Testimony of Professor Stephen Neale)

169. Some filters allow the user to block only certain categories, such as pornography and adult/sexually oriented materials; other filters do not allow for customization, but rather the user must select a predefined list of settings relating to a level of filtering or an appropriate age range. Mewett Report ¶ 39.

170. Internet content filtering software may be ineffective in two ways: underblocking and overblocking. Underblocking occurs when the filter fails to block content that would meet the filtering criteria (such as sexually explicit content). Overblocking occurs when the filter prevents access to material that does not meet the filtering criteria, resulting in the inaccurate blocking of, for example, political, social, and health-related Web sites. Mewett Report ¶ 37.

171. Difficulties both with underblocking and with overblocking have led some parents to become dissatisfied with filtering software, and have led them to discontinue the use of that software. According to a survey conducted by one major Internet service provider, one in five former users of parental controls reported that the reason they ceased using such controls is that they did not believe that these controls were effective. According to the same study, some parents have reported that they disabled their filters because their children could not access Web sites needed in order to do their homework. Mewett Report ¶ 37.

172. ContentProtect, CyberPatrol, CyberSitter, McAfee, NetNanny, and Norton were rated by TopTenReviews in the 2006 internet filter review as the best content filters on the market. Mewett Report ¶ 38.

173. Mr. Mewett performed tests of these filters, as well as filters offered by AOL and MSN, two internet service providers that offer a nationwide product. Mewett Report ¶ 38.

174. Several of the filter products propose to offer a range of settings to specify the type of material that the user hopes to block and not to block. In his tests, Mr. Mewett set the filter products at the settings that appeared to be the most likely to block sexually explicit material without blocking non-sexually explicit material. He also tested the filters at their default settings where applicable. Mewett Report ¶ 39.

175. Mr. Mewett tested the filters against data sets of URLs, described above, consisting of random samples drawn from the Google and MSN search engine indices; URLs returned in response to a random set of searches on the MSN, Yahoo!, and AOL search engines; and URLs returned in response to the most popular searches as reported by the Wordtracker service. Mewett Report ¶ 50.

176. Mr. Mewett classified these URLs into several categories. One category was for web pages with no sexual content. The first category of web page was tested to determine the frequency at which the filter products block non-sexually explicit web pages. A second category was for sexually explicit web pages for which the apparent primary purpose was only adult entertainment. Web pages with a different apparent primary purpose, such as an education, literary, or health-related purpose, were not included in this category. The second category of web pages was tested to determine the frequency at which the filter products fail to block sexually explicit web pages. Mewett Report ¶¶ 58, 63.

177. Dr. Stark performed a statistical analysis of the results of this testing. With regard to the sets of web pages drawn from the Google and MSN search engine indices, Dr. Stark's analysis found that the various filter products failed to block the sexually explicit web pages from 8.6 percent to 60.2 percent of the time. The various filter products blocked the non-sexually explicit web pages from 0.4 percent to 23.6 percent of the time. (Stark Report ¶ 11.) As a general rule, the more that a particular filtering product overblocked, the less that it underblocked, and vice versa. None of the products had a combined underblocking and overblocking score that was less than 16.3 percent. (Stark Testimony)

178. With regard to the web pages that were returned from a random sample of queries on the MSN, Yahoo!, and AOL search engines, Dr. Stark's analysis found that the various filter products failed to block the sexually explicit web pages from 6.2 percent to 43.4 percent of the time. The various filter products blocked the non-sexually explicit web pages from 0 percent to 20.7 percent of the time. (Stark Report ¶ 11.) Again, as a general rule, the more that a particular filtering product overblocked, the less that it underblocked, and vice versa. None of the products had a combined underblocking and overblocking score that was less than 14.8 percent. (The two

products with a 0 percent overblocking score also underblocked sexually explicit web pages at rates of 20.4 percent and 43.4 percent, respectively.) Among the queries that retrieved at least one sexually explicit web page, between 15.6 percent and 56.1 percent of those queries retrieved at least one sexually explicit web page that was not blocked by the various filters. (Stark Testimony)

179. With regard to the web pages that were returned from the most popular queries as reported by Wordtracker, Dr. Stark's analysis found that the various filter products failed to block the sexually explicit web pages from 1.3 percent to 12.6 percent of the time. The various filter products blocked the non-sexually explicit web pages from 2.9 percent to 32.8 percent of the time. (Stark Report ¶ 11.) Again, as a general rule, the more that a particular filtering product overblocked, the less that it underblocked, and vice versa. None of the products had a combined underblocking and overblocking score that was less than 13.1 percent. (Stark Testimony)

180. Overblocking is a significant concern. Because non-sexually explicit web pages were significantly greater in number in Mr. Mewett's and Dr. Stark's study than were sexually explicit web pages, even a relatively small increase in the percentage of "clean" web pages that are blocked can result in many blocked pages for a typical user.

181. Examples of non-sexually explicit web pages that were blocked by the filters tested by Mr. Mewett include the following: www.nakedjuice.com (a fruit juice company); www.topless-sandal.com (a footwear company); www.boobiethon.com (a breast cancer awareness web site); www.aclufl.org/news_events/calendar/index.cfm?viewDate=6%2F1%2F2005 (the calendar of a state ACLU chapter); www.cia.gov/cia/publications/factbook/geos/mx.html (the CIA World Fact

Book); www.i-love-cats.com; and www.weightlossguide.com. Mewett Report ¶ 80; Mewett Rebuttal Report ¶ 12.

182. Even websites maintained by the Plaintiffs are subject to overblocking. For example, www.powells.com, an online bookstore, was blocked at the domain level in its entirety by four of the filters, and certain pages were blocked by an additional four filters. All but two of the filters blocked, either entirely or partially, www.scarleteen.com, a web site operated by Heather Corrina Rearick that is apparently designed specifically for teenagers. In addition, www.sexualhealth.com, a sex education web site, was blocked either entirely or partially by every filter setting tested. Two of the filters blocked all of the plaintiffs' web sites. Mewett Rebuttal Report ¶ 17.

183. A substantial portion of the sexually explicit web pages that were not blocked by the filters are hosted in the United States. For the sets of web pages randomly drawn from the Google and MSN search engine indices, Dr. Stark's analysis found that between 31.6 percent and 49.7 percent of the sexually explicit and not-blocked web pages in that data set were hosted in the United States, varying by filter. (Stark Testimony)

184. These percentages generally increase for the web pages that were returned from a random sample of queries on the MSN, Yahoo!, and AOL search engines. Between 33.8 percent and 91.9 percent of the sexually explicit and not-blocked web pages in that data set were hosted in the United States, varying by filter. (Stark Testimony)

185. Those percentages increase further for the web pages that were returned from the most popular queries as reported by Wordtracker. Between 69.2 percent and 96.6 percent of the sexually explicit and unblocked web pages in that data set were hosted in the United States, varying by filter. (Stark Testimony)

186. Most sexually explicit web pages that are hosted outside of the United States have a commercial link to the United States. The vast majority of those web pages either directly solicit subscriptions or sales from their customers, including customers in the United States, or link to a web site that does so. Of the sexually explicit web pages in the data sets tested by Mr. Mewett that were hosted outside the United States, but that did not directly solicit subscriptions or sales, approximately 90 percent of those web pages either contained images that were themselves hosted in the United States, or linked to a web site that solicits subscriptions or sales. Specifically, 90.3 percent of the web pages in the Google index data set did so, 89.8 percent of the web pages in the MSN index data set did so, 88.2 percent of the web pages in the random search engine query data set did so, and 95.9 percent of the web pages in the Wordtracker query data set did so. Stark Rebuttal Report ¶ 26.

187. These estimates likely understate the prevalence of sexually explicit web pages and the rates at which filters fail to block sexually explicit web pages or block non-sexually explicit web pages. For example, Dr. Stark counted queries that did not retrieve any working websites in the denominator of estimates of the prevalence of sexually explicit material. Further, the definition of a sexually explicit web page that was used for the purpose of Mr. Mewett's and Dr. Stark's study is restrictive; in order to qualify, the page must have sexually explicit content that is clearly adult entertainment, and that content must be visible without clicking anything, not even the "play" button of a video. Similarly, the definition of a non-sexually explicit web page that was used for the purpose of this study is also restrictive; in order to qualify, the page must have no nudity or sexual content whatsoever. (Stark Report ¶ 20; Mewett Report ¶ 63)

188. In addition to the personal computer-based and ISP-based filtering products described above, certain search engines also offer filtering services with respect to searches

performed on those search engines. Any user, however, can disable a search engine filter with the click of a button; there is no password protection that would enable parents to ensure the filter is set at all times. Mewett Report ¶ 65.

189. Mr. Mewett tested filtering products offered by three search engines – Google, Yahoo!, and Verizon – by running the one hundred most popular search terms, as reported by Wordtracker, through those search engines. Even with the search engine filter setting activated, 3 percent of the top 100 Wordtracker queries returned sexually explicit web pages for Google; 8 percent returned sexually explicit web pages for Yahoo!; and 10 percent returned sexually explicit web pages for Verizon. This is a conservative test, because it is likely that search engine filters would focus their efforts on the most popular queries. Mewett Report ¶ 69.

190. Search engine filters face significant overblocking difficulties. For example, Google SafeSearch consistently blocks web sites operated by the U.S. government, by American newspapers, and by Fortune 1000 companies. Furthermore, Google SafeSearch frequently blocks even web sites that are specifically targeted at, or are helpful to, children. Mewett Report ¶ 79.

191. The Plaintiff retained J. Christopher Racich of First Advantage to perform a study of the effectiveness of internet content filtering software. He tested four filtering products, but only submitted expert reports with respect to two of those products. He tested each of those products with respect to their efficacy at blocking sexually explicit material, but he did not test those products in any way with respect to their efficacy in avoiding the blocking of non-sexually explicit material.

192. Mr. Racich tested the Safe Eyes 2006 brand of filtering software, and set that product to attempt to block all of its default categories, including “nudity,” “pornography,”

"sex," and "tasteless/gross," and also to attempt to block the additional categories of "adult" and "lingerie."

193. Mr. Racich tested the 8e6 Home Internet Protection Services brand of filtering software, and set that product to attempt to block all of its default categories, including "obscene," and "r-rated."

194. Although Mr. Racich did not disclose these additional tests in his expert reports, he also tested the CyberPatrol filtering software (at both its "mature teen" and "young teen" settings) and the Net Nanny filtering software. In those tests, the Cyber Patrol software failed to block 304 out of 1267 sexually explicit web pages (as identified in Mr. Mewett's study) at its "mature teen" setting, and failed to block 284 out of 1264 sexually explicit web pages at its "young teen" setting. The Net Nanny software failed to block 311 out of 1265 sexually explicit web pages in Mr. Racich's test.

195. Internet content filtering software works more efficiently in a corporate or institutional workspace than it does in a residential setting. A corporate client would have the budget to employ the correct people to install and manage the filtering systems. In addition, the corporate client likely would want to ensure that its employees only have access to what is deemed to be necessary for productivity, and thus would wish to allow only a relatively smaller category of websites to be permitted. In contrast, a parent is more likely to have a limited budget, limited knowledge, limited time, and non-standardized hardware and software. Mewett Report ¶ 72.

196. The figures that are reported as the results of Mr. Mewett's and Dr. Stark's study reflect the likelihood that a filter, if installed and in proper working order, would block sexually explicit material. However, not all users employ filters. Parents may choose not to use a filter

because they find the software to be too restrictive, limiting the child's ability to research online effectively. Mewett Report ¶ 74.

197. A customer must have a significant degree of computer knowledge, and be willing to undertake a certain degree of effort, in order to install, configure, and update filters. An inexperienced parent is likely to face difficulties in installing the software or in attempting to remove it at a later date. Many computers are unable to effectively utilize filters due to technical constraints and compatibility problems, such as firewalls or anti-virus software. Mewett Report ¶ 74.

198. Internet filters can be circumvented. There are many web sites available that describe how to disable or to circumvent specific filters, as well as filters in general. In some cases, it is possible to access these instructions even while the respective filter is turned on. For at least four of the filters that Mr. Mewett tested, he was able to obtain instructions from the Web on how to disable or bypass that filter, even with the filter turned on. For example, he was able to find a document at www.cexx.org/censware.htm outlining two methods for bypassing the Net Nanny filter by typing "disable net nanny parental controls" into the Google search engine with the Net Nanny filter on. Mewett Report ¶ 74.

199. Web proxy sites can be used to gain access to Web sites that have been blocked. A proxy server allows clients to make indirect network connections to other network services. An example of a readily-available web site that instructs viewers on how to use proxy sites to circumvent filters is found at www.zensur.freerk.com. Mewett Report ¶ 74.

200. Translation tools may also be used to access sexually explicit Web sites in foreign languages. Sexually explicit search words may be typed in English into tools such as Google translation, and the translated into a different language, resulting in a list of foreign URLs that

likely can be accessed without being blocked by a filter. This is because most filtering is done through the use of English phrases. Mewett Report ¶ 74.

201. Some search engines use a technique called "cache," which permits a user to view a previous version of a web page if that page has changed after it is first found by the search engine's web crawler. Some filters may block a link to a particular web site with sexually explicit content, but would not block a cached image of that site. Mewett Report ¶ 74.

202. Filters do not necessarily block a certain URL every time that that URL is entered into a browser. In other words, a claimed success rate of 80 percent in blocking sexually explicit content does not entail that 80 percent of all content is always blocked; instead, the same content may be blocked 80 percent of the time and allowed 20 percent of the time. Mewett Report ¶ 74.

203. The conversion of residential households in the United States to broadband Internet connections will exacerbate the limitations of Internet content filtering software. Some personal computers will not be upgraded, but will be expected to cope with the increased volume of data made available at higher speeds through broadband connections. Mewett Report ¶ 74.

204. Redirected URLs also pose a difficulty for Internet content filtering software. Pornography merchants frequently acquire new or expired domains, with the intention of automatically forwarding the viewer of those domains to one or more of the merchants' own pornographic URLs. Pornography merchants have developed mechanisms through which hundreds of pornography URLs are rotated sequentially. Mewett Report ¶ 74.

205. Commercial pornography merchants also have stolen metatags from non-pornogrpahic web sites. Because search engines use the metadata of a web page to determine the content of that page, the pornography merchants' use of this stolen metadata would prevent a search engine from identifying the page as sexually explicit, and may cause the search engine to

direct a viewer to that site even if the viewer enters a search for non-pornographic material. Mewett Report ¶ 74.

206. None of the products that Mr. Mewett tested attempted to block web pages through an analysis of the images on the page. It is extremely difficult to identify images, or to categorize images as sexually explicit, through automated software. Home personal computers currently lack the capacity to support software that would have that capability. Since filtering software relies instead on analysis of words and phrases, a pornography merchant can evade the software by placing text on the web site in the form of images. Mewett Report ¶ 74.

207. Many sexually explicit web pages do not use metatags, because the purveyors of those web sites do not wish the sites to be identified by the search engines as sexually explicit. Mewett Report ¶ 75.

208. Internet content filtering software tends to be low-level software. The software is designed to install itself between the normal applications on a computer and the transport and protocol layers of the operating system's network communications. Software is not ordinarily installed at this level of the operating system. The potential therefore exists for the code of another program to conflict with the filtering software at this level, with adverse consequences for the entire operating system. Mewett Report ¶ 76.

209. Because filtering software generally is designed to be secure, any attempts to uninstall or reconfigure the software may be interpreted by the program as an attempt to circumvent it. This could result in invalid configurations that will render the computer unusable or unable to connect to the Internet. Mewett Report ¶ 76.

1. Limitations of Technology (Neale)

210. Filtering software is concerned with the problem of assigning Web pages to a set of predetermined categories. In this regard they are no different from systems and services that classify texts or images according to other properties, such as topic, genre, or type. (Neale Testimony)

211. All filtering software is premised on the assumption that the content of any Web page can be accurately classified by assigning it to pre-selected categories that filter companies consider useful. Typical categories include "travel," "health," "sports," "employment," "finance," "shopping," "personals," "drugs,"and "pornography." (In this regard, they are no different from systems and services that classify texts or images according to other properties, such as topic, genre, or type). The number of categories tends to be in the range of thirty or so. Once the content of a Web page has been classified, it can be entered into a database of URLs and/or IP addresses under the category or categories to which it has been assigned. Neale Report ¶ 3.1

212. When configured to block access to sexually explicit material, filtering software blocks a substantial amount of material on the Web that is not sexually explicit or fails to block material that is sexually explicit. Filtering software is intrinsically unable to block sexually explicit material while simultaneously allowing minors access to all protected speech because all filtering involves an immutable trade-off between the overblocking caused by aggressive filter settings and the underblocking caused by more liberal settings. (Neale Testimony)

213. Filter companies acknowledge that the proportion of pages from customers is quite limited. Moreover, the filter companies acknowledge that the overall impact of this information on the size and quality of databases is not significant. Neale Expert Report, ¶ 3.3.5.

214. List-based filtering, or the use of "black lists" is generally limited in two ways: (i) not all of the theoretically indexable Web is indexed, and (ii) a significant number of web pages reside in the Deep Web, which is invisible to the spidering, list-gathering techniques employed by search engines and filtering technology. Neale Expert Report, ¶ 4.2.1.

215. Dynamic filters must be able to detect and respond to features in Web pages that are considered indicative of content. For the most part, this means features of the text in Web pages such as the presence of "keywords" and potentially revealing word distributions, which may be determined by statistical analyses. Neale Expert Report, ¶ 4.2.2.

216. In linguistics, the philosophy of language, the philosophy of mind, cognitive science, logic, computability theory, and information science, a crucial distinction is made between the form and the content of an expression. To talk of the form of an expression — a word, a phrase, or a sentence — is to talk about that expression without regard to its meaning/interpretation/content. The form of an expression can be recognized without knowing anything whatsoever about its meaning (interpretation, content). In such scenarios, you have been trained to respond to form not to content. Recognizing form takes place without any understanding of content. Neale Expert Report, ¶ 5.1.2.

217. Classification/filtering software classifies Web pages on the basis of form not content. Specifically, it classifies on the basis of formal features it has been programmed to recognize and perhaps weight. These formal features are meant to indicate, with certain probabilities, the presence of types of content humans recognize and understand. Neale Expert Report, ¶ 5.3.2.

218. Web pages are basically text documents, often with files embedded in them (*e.g.*, image files, video files, or sound files). Neale Expert Report, ¶ 4.2.2.

219. The text in a Web page consists of (a) the text visible in the Web browser window, (b) the text making up the page's URL (*e.g.*, www.hotvixens.com), (c) the text used in specifying links (*e.g.*, "Click here for more pussy pics"), (d) the text making up the names of embedded files (*e.g.*, blowjob32.jpg, pamelaorgasm5.mp3, pamsuckingtom.mpeg), and (e) any HTML markup used to create the page, visible or not. Neale Expert Report, ¶ 6.1; Neale Testimony.

220. A filter that responds to the text making up the name of an image file (*e.g.*, blowjob03.jpg) is a text-based filter, not an image-based filter. Similarly, filters that respond to the text making up the names of audio files (*e.g.*, screamingorgasm.mp3) or video files (*e.g.*, blowjobs.jpeg) are text-based filters (not audio-based or video-based filters).

221. No commercial filtering software exists that classifies Web pages by recognizing and weighting features of audio or video files. (Neale Testimony)

222. Image-based classifiers/filters perform much worse than text-based classifiers/filters. Thus text-based classifiers form the core of current commercial filtering technology. To this extent, the effectiveness of current filtering software is largely a function of how well it manages to differentiate textual features and recognize connections among them. (Neale Testimony)

223. For the purposes of current text-filtering software, a text is nothing more than an unordered collection of words (and, in some cases, part words and near words) with no syntactic structure imposed upon them. So no difference is registered between, for example, "the dog chased the cat" and "the cat chased the dog," even if though the sentences have different meanings. (Neale Testimony)

224. No such list of keywords (or key strings) can provide necessary and sufficient conditions for correct classification: words on any list can appear on Web pages that clearly should not be considered under a specified category; and pages that clearly should be classified as falling within a category need contain no word from that list. The more one expands the list so as to block more sexually explicit or pornographic sites, for example, the more one will overblock, *i.e.*, block non-explicit non-pornographic sites; and the more one contracts the list to reduce overblocking, the more one will underblock, *i.e.*, fail to block sexually explicit or pornographic sites. This relation between overblocking and underblocking is immutable. (Neale Testimony)

225. A mere string of words is not a sentence or even some smaller phrase. Phrases have syntactic structure. (Neale Testimony)

226. A search conducted by filtering software for a mere string of words is far more coarse-grained than a search for a constituent made up of exactly those words in that order, and this can lead filters to overblock web pages that do not contain sexually explicit material. (Neale Testimony)

227. A filter that is blind to phrase structure will tend to underblock pornographic images. (Neale Testimony)

228. Classifying text without the means to assign phrase structure to it will not be effective. More sophisticated representations than unordered collections of words could be used by classification/filtering software, and it appears that some such software does use small numbers of short strings. But filtering software does not use, and, in light of the computational and comprehensional limits of filtering software, could never make use of anything like the

sophistication of the structures that generative linguistics has discovered humans actually invoke in understanding the meaning of phrases or sentences. (Neale Testimony)

229. There are at least three different notions of context that are relevant to discussions of the classification of content: (a) linguistic context, (b) formal context, and (c) context of interpretation. (Neale Testimony)

230. Automated systems are not currently able to replicate either the psychological complexity and creativity or the real world knowledge and perceptual, emotional, and social experience at the core of both the capacity to use and interpret language, and our capacity to understand the linguistic and non-linguistic behavior of one another. (Neale Testimony)

231. Computers are able to perform tasks that essentially consist of calculating probabilities and generally crunching numbers. What they can not do, and will never be able to do, is abstract features of sorts they have not been programmed to recognize, or form novel hypotheses about the world, or draw on a rich background of perceptual, emotional, and social experience that can be obtained only by living in the world and seeing how others with the same general physical and cognitive architecture live in it. (Neale Testimony)

232. Filter companies refer to “neural nets” and “artificial intelligence” playing key roles in their statistical classifiers. However, while these references suggest a degree of “intelligence” that resembles or mimics human intelligence, understands patterns, or learns a language, such references are metaphorical only. (Neale Testimony)

233. A neural net is essentially a family of algorithms, and the use of the word “neural” does not mean that the algorithms (or the overall system using them to determine such things as weightings) learns or understands or sees things in the way humans do. (Neale Testimony)

234. The effectiveness of filters are typically assessed by standard mathematical measures (and terms for these measures) in information retrieval. They involve measures of precision, which translates to a measure of overblocking, and recall, which translates to a measure of underblocking. (Neale Testimony)

235. Precision is measured by the proportion of the things a classification system assigns to a certain category that are appropriately so classified. (Neale Testimony)

236. Recall is a measure of the proportion of the actual members of a category the classification system identifies. (Neale Testimony)

237. Recall and precision are inversely related; that is, an increase in one is accompanied by a decrease in the other. Thus, for example, devising a method to capture every Web site that may fall under the criteria for a given category – thus maximizing recall — would likely also capture a relatively high proportion of Web sites that do not belong in the category — thus degrading precision. Conversely, devising a method to focus on highly accurate classification by whatever method — in order to maximize precision – would likely result in the failure to locate all Web sites that ought to be in the category — thus diminishing recall. This tradeoff is intrinsic to the problem, which means that no one method offers a perfect solution and no one filter is, or can be, without deficiency. (Neale Testimony)

238. In automated classification, there is always a trade off between precision and recall. (Neale Testimony)

2. Market Failure (Eisenach)

239. The percentage of children ages 3-17 using the Internet from home increased from 11 percent in 1997 to 42 percent in 2003. Eisenach ¶¶ 5, 26 at Table Three.

240. Approximately 41 percent of Internet-connected households have children. Eisenach Dep. at 141:24-142:3.

241. The potential market for home-based Internet content filtering software ("filtering software") is the 41 percent of Internet-connected households with children. Eisenach Dep. at 141:24-142:6.

242. Market survey evidence suggests that approximately four out of ten Internet-connected households with children use filtering software. Eisenach Principal Report ¶ 8.

243. Market penetration refers to the frequency of adoption of a product by consumers. Eisenach Dep. at 262:9-11.

244. The level of market penetration of filtering software indicates a failure of the market to provide products which are effective and can be effectively used by consumers. Eisenach Dep. at 264:9-22.

245. A significant proportion of households that do not use filtering software are deterred from using it, or have tried to use it and stopped, because they find the available products to be too complex, too ineffective, or a combination of the two. Eisenach Principal Report ¶ 9; Eisenach Dep. at 58:4-18.

246. The costs of using filtering software include the time parents must spend installing, setting up and maintaining the software, which for many parents, is a significant deterrent to filtering software use, and for some, an insurmountable one. Eisenach Principal Report ¶ 109.

247. Filtering software products are more difficult to install than word processing products. Eisenach Dep. at 192:6-8.

248. Filtering software products are more difficult to use than other types of software. Eisenach Dep. at 300:4-19.

249. The primary providers of filtering software are computer security software companies, broadband content providers, and Internet service providers. Eisenach ¶ 7.

250. Filtering software is the only software that allows children to access the Internet while not having access to inappropriate material. Eisenach Dep. at 68:13-23.

251. Among reasons parents are deterred from using Filtering software are that filtering software causes over blocking and under blocking, and can be circumvented by children. Eisenach Principal Report ¶¶ 119-125.

252. The nature of filtering software and market are conducive to market failure because of the asymmetry of information between consumers and producers of the filtering software. Eisenach Dep. at 56:3-56:10.

253. The market for filtering software is smaller than the market for other kinds of security software, thereby causing filtering software producers to have weaker incentives to improve the quality of their product, and contributing to market failure. Eisenach Dep. at 56:11-56:18.

254. A market failure exists when the value to consumers of higher quality products, if produced, would exceed the cost of producing them. Eisenach Dep. at 269:12-17.

255. Neither the price nor the cost to the consumer of filtering software is a substantial deterrent of the use of filtering software. Eisenach Dep. at 57:24-58:2.

256. Filtering software is sometimes available to parents for free. Eisenach Dep. at 61:19-62:21.

257. There is a demand for good filtering products that is not being met. Eisenach Dep. at 200:12-18.

258. It is unlikely that better filtering software for home computers will be developed because the market is not large enough for the product. Eisenach Dep. at 141:17-141:23.

259. The lack of some parents' technological sophistication is a factor that contributes to some parents' failure to use filtering software. Eisenach Dep. at 206:4-16.

260. Survey data shows that fewer than one-half of Internet-connected households with minor children presently use filtering software on their home computers. (Eisenach Testimony)

261. Families do not use filtering software for many reasons, including the following: (1) the burden and complexity of installing and using filtering software; (2) frustration with the under- and over-blocking of content; (3) the ability of children to circumvent filtering software; and (4) low demand for the product leaves producers with little incentive to create and market a high-quality product. (Eisenach and Mewett Testimony)

262. Producers lack an incentive to create a quality product because consumers make purchases without assessing the quality of the product. When consumers use the product, they are unable to determine whether the product is good or bad. Therefore, the filter market is stuck with no incentive to develop a better product. This is known as the "Lemons problem." (Eisenach Testimony)

263. In such markets, producers of high quality products are unable to obtain full value for the products they produce, since consumers are unable to distinguish high quality products from low quality products, and therefore are unwilling to pay the full cost of producing a higher quality product. Eisenach Principal Report ¶ 133. *See also* George A. Akerlof, *The Market for*

"Lemons:" Quality Uncertainty and the Market Mechanism, THE QUARTERLY JOURNAL OF ECONOMICS 84;3 488-500 (Aug. 1970).

3. Internet Content Filtering on Personal Digital Assistants and Mobile Phones

264. Alternative Internet access devices ("IADs") are rapidly penetrating the population of both adults and children. The Center for the Digital Future reports that 14.5 percent of those surveyed in 2003 reported accessing the Internet through a cell phone, wireless personal digital assistant ("PDA") or wireless computer, up from 9.2 percent in 2002. Eisenach Principal Report ¶ 44.

265. Many cell phones now include the ability to browse the Internet, and adult content providers are actively pursuing this market as an outlet for their materials. *Id.*

266. Filtering software has not been made commercially available that can be installed on non-PC internet access devices, such as cell phones or personal digital assistants. (Eisenach Report ¶ 124)

267. Carriers that offer mobile internet access do not offer filtering on their networks. (Eisenach Report ¶ 124)

268. It is not clear whether it is technically feasible to create effective filtering software for mobile devices, or when such software would be implemented. (Eisenach Report ¶ 124)

269. Traditional webpages are around 20K in size. Webpage designed for mobile phones average 1K to 2K in size because they are designed specifically for display on mobile phone screens and other portable devices. (Neale Testimony)

270. Mobile phone webpages create a problem for employees of filtering software companies who classify web pages because these smaller pages have fewer features that can be

sued to differentiate content. Consequently, problems with feature-driven classification are magnified in the classification of webpages for mobile phones. (Neale Testimony)

D. Other Alternatives

271. For the purposes of this litigation, the Plaintiffs do not contend that the creation of a top-level domain name for sexually explicit websites would be a less restrictive alternative to the requirements of COPA.

272. Top-level domains must be established by the Internet Corporation for Assigned Names and Numbers ("ICANN"), an independent international organization. ICANN has rejected a proposal to create a ".xxx" domain.

273. Even if a ".xxx" domain were created, it likely would generate many of the same objections raised in the present litigation. (Russo Dep. 28:18 - 29:21)

274. The creation of new Internet domains such as ".xxx," will not prevent minors from accessing harmful materials. (Russo Dep. at 26:24 – 27:17)

275. A separate child-friendly Internet domain such as ".kids" will not prevent the conveyance of harmful material to children. There is no need to speculate on the effectiveness of having a child-friendly Internet domain, because Congress authorized a second-level domain in 2002, *see* 47 U.S.C. § 941, and ICANN administers a top-level ".kids" domain. Website operators have responded without enthusiasm, and high costs and an overall lack of interest have rendered the domain a "ghost town," with only eight live websites two years after Congress authorized the domain. David McGuire, *Firms Ignore Kids-Only Internet Domain*, WASHINGTON POST, Feb. 20, 2004.

276. As of September 29, 2006, the top-level domain name "www.kids.us" contained 22 websites. One of those websites is an index for the other sites. Two of those websites are defunct.

277. A review of the history of obscenity prosecutions demonstrates that websites that have been prosecuted as obscene include, *inter alia*, depictions of feces smeared on women's breasts and genitals, child pornography, depictions of bondage and sadistic or masochistic behavior involving children, sexual contact between an adult woman and a dog, violent gang rapes of women, sexual intercourse between humans and other animals, and sexual activity involving urination, defecation, or genital mutilation. (Def.'s 2d Supp. Response to Pls.' Contention Interrog. No. 18 (Sep. 27, 2006))

III. COPA'S REQUIREMENTS

278. Congress has provided several affirmative defenses to COPA to ensure that adults can access material deemed harmful to minors, while restricting minors from access to such speech. It is an affirmative defense under COPA for a website to restrict access by minors to material that is harmful to minors by requiring the use of a "credit card, debit account, adult access code, or adult personal identification number," "by accepting a digital certificate that verifies age," or by "any other reasonable measures that are feasible under available technology." 47 U.S.C. § 231(c)(1).

A. Payment Cards

279. "Traditional payment cards" refer to a credit card, debit card, and prepaid card (reloadable version only) issued by five card companies (*i.e.*, American Express, Diners Club, Discover, MasterCard Visa): (1) personal credit are essentially a loan from a financial institution to an individual or a company to make purchases with or obtain cash advances; (2) debit cards

allow cardholders to access funds in their checking account to obtain cash and make purchases; (3) prepaid debit cards allow individuals to purchase a payment card and "pre-fund" it with cash or funds from one of their own credit cards and then use the prepaid debit card to obtain cash or make purchases (*e.g.*, gift cards, payroll cards, corporate incentive cards). (Clark Testimony)

280. "Traditional" payment cards (both credit and debit) are very popular and easy to use. The near universal view is that credit and debit cards are "easy and convenient" to use. There are three primary reasons why the traditional payment cards are so popular: (1) there is no dollar liability for the consumer; (2) most consumers have established these cards as their primary payment vehicle; (3) these cards bring "guaranteed" business to the website operators. (Clark Testimony)

281. In the U.S., adult ownership of traditional payment cards is widespread and these cards are easy to use. However, this is not the case for children, because card issuers, due to state laws, have always been reluctant to issue accounts to individuals under age 18. (Clark Testimony)

282. Each state has a law that defines the "age of majority." That is the age when an individual who enters into a contract can not be released from the commitment due to age. This is important to the financial institution to ensure that they can collect an outstanding balance (*e.g.*, credit card, debit card tied to a checking). Most states set the "age of majority" at 18. Five states have the age set higher than 18 (*e.g.*, Alabama 19, Indiana 21, Nebraska 21, New Hampshire 21, Pennsylvania 21). Further, some states allow individuals under 18 years old to be considered "age of majority" individuals under special circumstances (*e.g.*, Utah, any age if married). (Clark Testimony)

283. Most adults own either a credit card (*e.g.*, American Express, Discover, MasterCard, Visa) or a debit card tied to their checking account (*e.g.*, Discover, MasterCard, Visa). However, even "unbanked" adults can acquire and use reloadable prepaid cards to make purchases on the Web. Pursuant to the requirements of the Know Your Customer Provisions of the USA Patriot Act, issuing banks require a purchaser of a reloadable prepaid card to be an adult. (Clark Testimony)

284. About 80 percent of U.S. consumers (*i.e.*, 18 years and older) have made purchases online. Since 2001, consumer comfort with Internet purchasing has increased significantly for both credit cards and debit cards. (Clark Testimony)

285. Currently, 66 percent of consumers feel "comfortable" or "completely comfortable" with using credit cards for online shopping and 50 percent feel comfortable with using debit cards. (Clark Testimony)

286. Both the Pew Internet & American Life Internet Project study Teens and Technology (July 27, 2005) and the Teenage Research Unlimited Spring 2006 wave 47 study found that about 37 percent of teens ages 12-17 had made purchases online. (Clark Testimony) (Mann Dep. at 57:5-6.) When 17-year-olds were excluded from the Teenage Research Unlimited data, the study found that only about 30 percent of teens ages 12-16 made online purchases. (Clark Testimony) Mann Dep. at 103:14-15.

287. The Teenage Research Unlimited Spring 2006 wave 47 study questions and answers 17-20 are authentic and admissible. (Clark Dep. Ex. 9; Mann Dep. Exs. 2-5)

288. The Pew Internet & American Life study did not present any data that excluded 17-year-olds from their results, nor did it ask any questions or collect any data about how teens ages 12-17 paid for their online purchases. Mann. Dep. at 60:3-8.

289. The Teenage Research Unlimited study found that about 60 percent of teens ages 12-17 who made online purchases used their parents' credit cards, about nine percent used their parents' debit card, and about two percent used their own credit card. Mann Dep. at 105:24 – 107:12. When 17-year-olds were excluded, the study found that about 60 percent of teens ages 12-16 who made online purchases used their parents' credit cards, about seven percent used their parents' debit card, and about 1.6 percent used their own credit card. Mann Dep. at 107:17 – 108:7.

290. Of the 73.6 million children under age 18 in the U.S., only a few have payment cards. About 11 percent of children age 12-17 (25.5 million, U.S. Census) or 2.8 million children have either a credit card or debit card. These payment cards are either an "extra" card on their parent's account or a "parent co-signed" card in the child's name. An additional 2.8 million teens occasionally borrow their parents' credit cards to make occasional online purchases. (Clark Testimony). Professor Mann does not dispute that about 5.6 million minors have ready access with the explicit consent of their parents. Mann Dep. 119:13-17.

291. Parents can supervise their children's online transactions at the time of purchase.

292. Even if actual purchases made with these cards are unsupervised, parents can see their children's payment card purchases online two to three days after the purchase is made, and, in some cases, the same day. Clark Testimony. Mann Dep. at 70:10-11.

293. Virtually all adult cardholders are familiar with reviewing a billing statement, and with calling the card issuer to inquire about unfamiliar or suspect purchases. Parents can thus monitor their children's online purchasing behavior. (Clark Testimony)

294. Commercial website operators that offer adult sexual content can process a zero-dollar transaction or charge a membership/access fee, but either transaction will appear on the card billing statement and allow the parent to supervise their children. (Clark Testimony)

295. Prepaid debit cards, also known as prepaid cards and stored-value cards, include "closed" system cards (such as store gift cards, cell-phone cards, transit cards), and "open" system cards that can be used at most merchants that accept these cards. Some cards are single purpose or non-reloadable and some are reloadable. The cards can be used to purchase goods/services and access cash at ATMs. A consumer can purchase and load these cards at a bank or retailer, over the phone or online. Usually there is a fee of $5-$8 per card; generally these cards are available in amounts up to $500. For reloadable cards, the Patriot Act requires that the card issuer collect certain information as part of the Patriot Act's "know your customer" provision (*e.g.*, name, address, phone number, birthdate). Based on the most recent data, "open" system cards represent less than 0.8 percent of the dollar volume in payment cards. (Clark Report)

296. The emergence of (non-reloadable) prepaid gift cards is not an obstacle to limiting children's access to harmful to minors material. (Clark testimony)

297. If a Web merchant can not successfully perform the two operational verifications now common for most online transactions (*i.e.*, billing address and CVC), the website operator is likely to decline that transaction. Since non-reloadable gift cards do not have a billing address and present a higher degree fraud risk, website operators can and generally will decline to accept these (non-reloadable) prepaid gift cards. (Clark testimony)

298. Reloadable prepaid cards have billing addresses due to the Patriot Act "know your customer" provision and therefore generally will be accepted by website operators. (Clark Testimony)

299. Although the growth of non-reloadable prepaid "gift" cards has been rapid, the vast majority of the growth has been with the "closed-system"products, such a Sears Gift Card. The size of "open-system" products, such as the Visa Gift Card, is minimal. (Clark Testimony)

300. Online merchants can decline to accept non-reloadable prepaid gift cards. (Clark Testimony)

301. The two primary Internet Payment Service Providers that control the adult entertainment market are CCBill.com and Paycom.net. Both CCBill.com and Paycom.net require a billing address in order to purchase access to online adult entertainment. (Russo Dep. at 75:9-14, 97:4-9)

302. Non-reloadable prepaid cards do not have a billing address. (Clark Testimony)

1. Existence of micro-payment technology to facilitate purchase of content (BitPass)

303. Bitpass was founded in 2002 to provide solutions that remove the roadblocks to digital content commerce and to allow digital media and entertainment companies to cash in on their content assets. Today producers and aggregators of digital media may want higher returns from investments in content. At the same time, rapidly changing consumer buying and usage behaviors may be redefining the digital media marketplace. Bitpass connects digital media producers with this growing market, offering solutions that increase return on content, customers and community. (Testimony of Douglas Knopper, CEO of Bitpass)

304. The Bitpass iMedia Commerce Engine marshals relevant delivery channels—including the web, cell phones, PDAs, MP3 players, podcasts and other digital media devices. (Knopper Testimony)

305. The Bitpass iMedia Commerce Engine offers digital media and entertainment companies a turnkey system built on open web standards and a software-as-a-service platform. The iMedia Commerce Engine supports rapid deployment, transparent web and commerce integration and secure financial transactions, consumer behavior tracking and seamless content and data integration. (Knopper Testimony)

306. Bitpass customers include leaders from media publishing, TV, film, radio, community and Internet and include segment leading firms such as Disney, Microsoft and MSN, Ziff Davis, Time, United Media, CanWest, and Entercom. (Knopper Testimony)

307. The iMedia Commerce Engine is available as an enterprise system or a self-service solution. Both products have access to the payment, security, fulfillment and analytics services of our high-availability technology platform. (Knopper Testimony)

308. Consumers use iMedia Account to purchase and access digital content on iMedia merchant sites. iMedia Account is a digital wallet application that offers consumers "frictionless" purchasing and complete privacy and anonymity. (Knopper Testimony)

309. iMedia Account is a "digital wallet" for the web. Consumers enter payment card, PayPal information, add some money the account and get single click purchasing. Consumers spend what's in the wallet and iMedia Account lets them know when they need to add more money. (Knopper Testimony)

310. Consumers pay with the funds in the account not the payment card information, which stays safe with Bitpass. iMedia does not require consumers to disclose personal information every time they make a purchase. (Knopper Testimony)

311. The iMedia Account has features for consumers to manage their accounts. Consumers can set purchase thresholds and track funding, purchases, log-in sessions and complaints and refunds. iMedia accounts are free to set up, have no monthly fees, and can be funded with as little as $3. (Knopper Testimony)

312. Bitpass makes the process of purchasing online content simple and convenient, without interrupting a website visitor's experience with the "flow" of the website. Purchases can be as little as $0.99, $0.10, or even for free. (Knopper Testimony)

313. Bitpass is ready to offer a version of its product to merchants that accepts only Bitpass accounts tied to a payment card. (Knopper Testimony)

314. Bitpass is developing a product that allows parents to monitor their children's Bitpass activity. (Knopper Testimony)

315. Bitpass is considering developing a product that would allow consumers to "purchase" content for free by watching a video advertisement. Such purchases will still require a Bitpass account and there will be a record of the purchase. (Knopper Testimony)

B. Age Verification Services

316. Age verification services can prevent minors from accessing harmful content. (Dancu Testimony and Dillon Testimony)

317. One technologically feasible manner in which websites can screen for age is through age verification services ("AVS products" or "AVS technologies"). AVS products, which currently are used for online wine and tobacco sales, require a consumer to enter personal

information—usually their name, address, and the last four digits of their Social Security number. The information is then verified using commercially available databases that aggregate public records. The process is completed in less than a second. (Dancu Testimony and Dillon Testimony)

318. AVS products are sophisticated enough to ensure that a customer is not using someone else's personal information. The AVS products generate questions based on personal historical information, such as the color of a given car or the address of a previous home. AVS companies tailor these quiz products to meet the needs of their consumers. Obviously, the more questions that are asked, the more effective the verification process. (Dancu Testimony and Dillon Testimony)

319. Age verification can be completed at little cost, which can be absorbed by the website operator. The cost, which currently ranges from as little as 25 cents to as much at $1.00, depending on the volume of transactions and the websites' tolerance level for errors, will drop dramatically when there is a high volume of transactions. An age verification password can be issued to certify that a consumer is not a minor and can be reused over a specified period of time on the same or different websites. (Dancu Testimony and Dillon Testimony)

C. Other Reasonable Measures That Are Feasible Under Existing Technology

320. In addition to existing methods of age verification, some promising "digital wallet" technologies are on the horizon, which can make online identity verification even easier than face-to-face verification, such as Microsoft's InfoCard and a competing product in development at the Berkman Center for Internet and Society.

321. Digital certificates are now technologically viable and are used by at least one bank.

322. Although age verification products are the most reliable existing method, the options for online identity and age verification are becoming more numerous, more effective, and increasingly inexpensive to implement.

D. Implementation of COPA Will Not Materially Affect the Web

1. Commercial Website Operators With Harmful to Minors Content Will Not Be Materially Affected

323. Testimony at the preliminary injunction hearing, including that offered by Professor Donna L. Hoffman, regarding the state of the Internet in 1998 and 1999 is irrelevant to the state of the Internet today because, as the Supreme Court recognized in *Ashcroft v. ACLU* (2004), the Internet has changed dramatically over the last several years. The Court accordingly directed that this Court undertake new fact-finding "to reflect current technological realities." 542 U.S. at 672.

324. Plaintiffs will not seek to introduce Professor Donna Hoffman's 2006 Expert Report on any live testimony from Professor Donna Hoffman because plaintiffs did not make Professor Hoffman available to defendant for deposition.

325. COPA will have no significant negative impact of commercial websites on the Internet. (Smith Testimony)

326. The Internet is a stable, established business communications tool, and COPA will not require the creation of a new business model. COPA will have no negative effect on commercial innovation or business models used in Internet commerce. (Smith)

327. In general, over 95 percent of commercial website operators in the U.S. accept traditional payment cards. (Clark Testimony)

328. Requiring the use of a payment card before website visitors can access adult sexual content on these websites places almost no burden on these merchants, (apart from the

potential costs of web redesign to segregate such content). Those few commercial websites operators that publish adult sexual content but do not yet accept payment cards, can select from three alternative approaches to process payment cards: (1) setup their own merchant account for traditional card payments; (2) use third party merchant account for traditional card payments; or (3) offer non-traditional payment vehicles like PayPal. The costs to honor the traditional payment cards are modest (generally between 2.5 percent to 5.5 percent of sales dollar volume), and even lower for PayPal. These costs, fraud and processing fees, are likely to decline over the next three to five years. (Clark Testimony)

329. Requiring the use of a payment card to view such content, however, "monetizes" a product that is in high demand. Requiring the use of a payment card is likely to reduce the number of website visitors. But such visitors were unlikely to make a purchase, and thus unlikely to affect business results. (Clark Testimony)

330. Moreover, requiring the use of a payment card should lead to repeat visits to the website where the website visitor has "registered" a payment card and/or obtained a membership for automatic access in the future. Thus, requiring the use of payment card should improve revenue levels. (Clark Testimony)

2. <u>Adaptability of consumers/Consumers are willing to provide personal information</u>

331. Internet commerce is thriving, which indicates that consumers are becoming increasingly comfortable with providing personal information on the Internet. (Smith Testimony)

332. Consumers are increasingly willing to register or provide a credit card in order to gain access to websites. (Smith Testimony)

333. COPA will not inhibit qualified consumers from viewing online content. COPA qualification standards, which require a password, registration or a purchase, are used successfully in many businesses where controlled products and services are purchased and consumed. (Smith Testimony)

334. Barriers are common in successful everyday shopping activities on the Internet. COPA's regulation of access to certain content by minors under the age of 17 will have no significant adverse effect on adults who access, search for information, or use the Internet. (Smith Testimony)

335. The modest burdens associated with COPA's affirmative defenses are analogous to the burdens associated with obtaining access to adult material in other settings, such as entries to nightclubs, adult bookstores, or NC-17 movies. *See Reno v. ACLU*, 521 U.S. at 890 (O'Connor, J., concurring in part and dissenting in part). (Smith Testimony)

336. Flow is caused by the nature of the content viewed and is not interrupted by the process of admission. (Smith Testimony)

337. Visually consumed products are traditionally paid for prior to consumption. Consumers pay in advance to see movies, Broadway plays or musical, art museum tours, and even national parks. Consumers expect to pay the required fee for visually consumed products prior to consumption. Because COPA requires qualification by methods other than credit card use, the merchant retains the option to not require purchase before a consumer views content. (Smith Testimony).

338. Consumers are willing to tolerate economic barriers in the form of time, inconvenience, or money to achieve a goal. From an economic perspective, this inelasticity of

demand may be high where loyalty to a product is high, or where the consumer derives sufficient value from the product. (Smith Testimony)

339. The pornography industry traditionally has faced both social and technological barriers that have not reduced industry demand. Every time a new medium for the dissemination of pornography is created, the technological advances have required not only a shift in consumer use behavior, but a shift in the business model within the industry. Yet there has not been a decrease in demand for the product category. (Smith Testimony)

340. The consumption of pornography requires a motivated user, one who actively seeks access to website pornography. The minimal qualification standards required by COPA are smaller than the barriers required to consume pornography through any other medium because the purchase can be made in the privacy of one's home. (Smith Testimony)

341. Visitors intending to purchase are not likely to be deterred by entering a payment card in order to access harmful to minors material because they are likely to still see the same benefits as before, such as convenience and anonymity. (Clark Testimony)

342. The Better Business Bureau and the Javelin Strategy & Research issued the 2005 Javelin Identity Fraud Survey Report. A summary of that report noted that: (1) the most frequent reported source of information used to commit fraud was a lost or stolen wallet or checkbook; (2) among cases where the perpetrator's identity is known, half of all identity fraud is committed by a friend, family member, relative, neighbor, or in-home employee; and (3) a wide variety of metrics confirm that identity fraud problems are not worsening, with the total number of victims in decline. (Smith Dep. Ex. 6)

3. Commercial Pornographers Easily Can Comply with COPA

343. There is no technical obstacle that would prevent commercial adult pornography sites from utilizing one or more of the screening mechanisms set out in COPA for limiting access to harmful to minors material.

344. Some commercial adult pornography sites do block all access to materials on their site unless and until a valid credit card or other form of adult identification (including adult password) is supplied; however, many adult pornography sites, numbering in the thousands, voluntarily choose to provide access to free sample images and texts. (H.R. Rep. No. 105-775, at 10. Russo Report)

345. COPA's affirmative defenses reflect Congress's understanding of the business model of commercial pornography to present "teasers" to garner business, and Congress's desire to ensure that the adult content is not contained in such publicly-accessible "teasers," but is restricted to the audience for which it is intended – adults. Congress noted that the affirmative defenses already "represent standard procedures for conducting commercial activity on pornographic Web sites," and that the affirmative defenses simply ensure that "the commercial pornographer . . . put sexually explicit images 'behind the counter.'" H.R. REP. NO. 105-775 at 15.

4. Plaintiffs Can Easily Comply with COPA

346. The Nerve.com website accepts payment cards on its premium membership subscription page. Membership is required to access most content on Nerve. Members get

> Hotter Photography. Photography so good, you could hang it in an art gallery — but so sexy, you'll be glad you can see it at home! An exclusive Premium-Members-Only gallery every week, featuring our hottest photos of naked women, men and couples.
> Interactive Nerve. Featuring uncensored videos, the monthly Amateur Photo Contest, the addictive on-screen crossword puzzle, and The Daily Siege weblog!

The website store on Nerve.com links users to Amazon.com, which accepts payment cards.

347. The Powell's Bookstore website accepts payment cards and the Powell's card, which is a form of gift card purchased with a payment card, to place an order.

E. Worldwide Solution

348. COPA applies to Web Site Operators who are not residents of the United States and who host a website server located outside of the United States but whose websites are viewable in the United States. (Def.'s Response to Contention Interrog. 34)

349. COPA applies to Web Site Operators who are residents of the United States and who host a website server located outside of the United States but whose websites are viewable in the United States. (Def.'s Response to Contention Interrog. 35)

350. COPA applies to Web Site Operators who are not residents of the United States and who host a website on a server located in the United States and whose websites are viewable in the United States. (Def.'s Response to Contention Interrog. 36)

351. The United States has entered into more than fifty bilateral Mutual Legal Assistance Treaties (MLATs) with other countries. These agreements provide the United States with the power, in investigating a violation of its laws that may have been committed by a resident of another country, to request the assistance of a signatory country to summon witnesses, to compel the production of evidence, to issue search warrants, and to serve process. *See, e.g.*, Treaty Doc. 105-12, 105th Cong., 1st Sess., Exec. Rpt. 105-22, 105th Cong., 2d Sess. (U.S.-Poland MLAT).

352. BetonSports PLC, a company organized under the laws of the United Kingdom; David Carruthers, its chief executive officer; ten other persons; and three other entities were

indicted by a grand jury in the United States District Court for the Eastern District of Missouri on June 1, 2006. The indictment charges several offenses, including the violation of 18 U.S.C. § 1804 for the transmission of wagers. In response to the indictment, the board of directors of BetonSports PLC announced that it would suspend its United States Internet wagering operations, which were physically based in Costa Rica and Antigua.

353. Each of the card companies (*e.g.*, Amex, Discover, MasterCard, Visa) have worldwide policies, operating rules and agreements, which govern any retailer or website operator worldwide that accepts payment cards. These agreements require compliance with all applicable laws and regulations. Further, if a website operator fails to comply with any applicable law, then the card companies can take one of several actions to correct this: impose increasingly severe fines and/or entirely rescind the right of the website operator to accept that company's payment card. (Clark Testimony)

354. Merchant agreements even require foreign merchants selling goods and services to U.S. customers to comply with U.S. laws. The card companies have taken this approach before for U.S. laws that were unique to the U.S. but important compliance regulations for a U.S. cardholder (*e.g.*, Fair Credit Billing Act/Truth & Lending Act). Thus, once COPA is in effect, foreign commercial adult sexual content providers will have to require use of a payment card before a visitor can view adult sexual content on their websites or risk fines or rescission of their right to accept cards. (Clark Testimony)

355. Recently, non-profit business and law enforcement communities announced the organization of the Financial Coalition Against Child Pornography. The Coalition, coordinated by two non-profit groups that focus on preventing child exploitation, brought together card companies, card processing companies, banks, and Internet companies such as AOL, American

Express, Chase, Citigroup Discover, First Data MasterCard, Visa, and Wells Fargo to set up a CyberTipline to identify website operators that sell child pornography, cut off their use of payment cards, and share this information with law enforcement communities. By identifying website operators that do not restrict access to adult sexual content, cutting off their use of payment cards, and sharing this information with law enforcement communities, the payment industry and law enforcement can target international commercial websites just as easily as domestic ones. (Clark Testimony)

356. Adapting the Financial Coalition Against Child Pornography to include COPA would essentially be a "fine tuning" process (*e.g.*, adding appropriate other non-profit agencies, adding appropriate new members, as well as adjusting operating tactics to focus also on commercial website operators that provide adult sexual content). The net result would be that children's access to adult sexual content (adult sex acts and content) would be targeted for control and enforcement. (Clark Testimony)

357. Child pornography is rarely posted on websites, either domestic or foreign, because the purveyors of that material are attempting to avoid enforcement efforts. Zook Report at 3; Zook Deposition at 46-47.

1. Due to geographic screening technology, the Internet is not necessarily global

358. Founded in January 2000, Quova, Inc. is the authority on intellectual property Intelligence and the leading provider of IP geolocation data and services to online businesses, including five of the world's six largest global Internet companies. Quova's patented technology provides the geographic location of website visitors in real time, enabling businesses to detect fraud, manage digital rights, target content, conduct site analysis and ensure regulatory compliance. Quova's customers and partners include such industry leaders as Major League

Baseball Advanced Media, BBC, Bell Canada, Cisco Systems, Coremetrics, Corillian, PassMark, Bankinter, Globo, Times Online and Sky Sports. (Testimony of Marie Alexander, President and CEO of Quova)

359. Quova is used to comply with FFIEC guidance, the Office of Foreign Assets Control (OFAC) regulations, the USA PATRIOT Act, and the Bank Secrecy Act, each of which have made knowing the location of online bank and credit union customers more important than ever. Quova is also used by the pharmaceutical, software, and online gaming industries, each of which are subject to regulations restricting where they can offer their products and services. (Alexander Testimony)

360. Quova can be used for content localization to customize website content to reflect the cultural preferences and priorities of online visitors from different regions and different countries. (Alexander Testimony)

F. Communications on the World Wide Web

361. It is technically possible to convert a web site delivered over the HTTP protocol to the FTP protocol. However, it is unlikely that all of the existing code on the site would work without modification. This is particularly true if the web page has embedded CGI scripts, which are the most common way for Web servers and Web browsers to handle information from HTML forms on Web pages. Mewett Rebuttal Report ¶ 25.

362. A web site operator who wishes to convert his site from HTTP to FTP would likely need to maintain at least some of the pages on the web site in HTTP, with traffic moving between the HTTP pages and the FTP pages. Mewett Rebuttal Report ¶ 25.

363. There may be complications for the viewer if a web site is converted to FTP. FTP requires specific ports, ports 20 and 21, to be left open to facilitate the connection. Some work environments, and even firewalls in domestic environments, may have these ports closed, rendering the web site inaccessible. In addition, firewalls may time out during large data transfers from FTP sites, causing an error to be generated. Mewett Rebuttal Report ¶ 25.

364. It would be important for a web site operator to ensure that the viewer of his site does not need to learn new Internet browsing skills to access his site. It is likely, however, that the conversion of a web site to FTP would require the viewer to reconfigure a firewall to confirm that the necessary ports are open for FTP. In addition, the viewer would need to change to a convention of typing "FTP://" in a browser bar, which would likely create confusion as browsers currently assume that a viewer intends to access HTTP and will automatically insert "HTTP://" in front of a domain name that is entered into a browser bar. Mewett Rebuttal Report ¶ 26; Felten Dep. at 54:8-12.

365. Search engines only index HTTP sites, and so simply entering a search term in the search engine will not return an FTP site. A viewer would either need to know the exact address of an FTP site to access it, or the web site operator would be required to maintain an HTTP site to direct viewers to the new site. Mewett Rebuttal Report ¶ 27.

366. Security concerns would likely deter web site operators from converting to FTP. That protocol is not designed for sharing sensitive information, such as a viewer's financial information. It is therefore likely that a commercial web site operator who operates an FTP site would revert to the HTTPS protocol for the purpose of processing sensitive information, rather than converting the web site entirely to FTP. Mewett Rebuttal Report ¶ 28.

III. Relief Sought

Plaintiffs seek a declaration that the challenged statute, the Child Online Protection Act (COPA), 47 U.S.C. §231, is unconstitutional, and a permanent injunction against its enforcement.

IV. Legal Issues

A. Plaintiffs'

1. Is COPA unconstitutional because it deprives adults of speech to which they are constitutionally entitled? *Reno v. ACLU*, 521 U.S. 844 (1997); *Butler v. Michigan*, 352 U.S. 380 (1957).

2. Is COPA unconstitutional because it is not narrowly tailored to a compelling governmental purpose? *Reno v. ACLU*, 521 U.S. 844 (1997); *Ashcroft v. Free Speech Coalition*, 122 S.Ct. 1389 (2002); *Ashcroft v. ACLU*, 524 U.S. 656 (2004).

3. Is COPA unconstitutionally vague? *Reno v. ACLU*, 521 U.S. 844 (1997).

4. Is COPA unconstitutionally overbroad? *Reno v. ACLU*, 521 U.S. 844 (1997).

5. Does COPA violate the First Amendment rights of older minors? *Reno v. ACLU*, 521 U.S. 844 (1997).

6. Does COPA violate the right to receive speech anonymously? *McIntyre v. Board of Elections Comm'n*, 514 U.S. 334 (1995); *Lamont v. Postmaster General*, 381 U.S. 301, 307 (1965); *Denver Area Educational Telecommunications Consortium, Inc. v. FCC*, 518 U.S. 727, 754 (1996); *ACLU v. Johnson*, 4 F. Supp. 2d 1029, 1033 (D. N.M. 1998).

Plaintiffs will fully address the legal issues in the pretrial memorandum.

B. Defendant's

1. Whether each Plaintiff has standing.

2. The standard of scrutiny to be applied to COPA.

3. The interpretation of the statutory language of COPA, including whether COPA has extraterritorial application.

4. Plaintiffs' First Amendment overbreadth challenge to COPA, on its face and as applied.

5. Plaintiffs' First Amendment vagueness challenge to COPA.

6. Whether Plaintiffs have a right to communicate and access information anonymously over the Web.

7. Whether older minors have a right to access harmful-to-minors material, as defined by COPA.

Defendant has addressed the issues of standing, anonymous speech, and Plaintiffs' claim regarding older minors in his Motion to Dismiss and, in the Alternative, for Partial Judgment on the Pleadings.

Defendant will address the remaining issues in his trial brief, in his proposed conclusions of law, and at trial.

V. Witnesses

A. Plaintiffs' witnesses

Pursuant to Fed. R. Civ. Pro. 65(a)(2), all prior evidence admitted in connection with the Temporary Restraining Order and the Preliminary Injunction are part of the record of this proceeding and may be cited by either party.

1. Plaintiff Rufus Griscom
   Nerve.com, Inc.
   520 Broadway, 6th Fl.
   New York, NY 10012

Mr. Griscom is the founder and publisher of a Web site called Nerve.com. He will testify to the nature of his Web site and the sexual content of the speech. He will testify that he fears prosecution under COPA for that speech and will explain the reasons for that fear. He will testify that there are other speakers on the Web who engage in similar speech, some of whom may be beyond the reach of COPA. He will testify that he could not operate his Web site with its existing content according to his best editorial and business judgment if he had to place all of the sexual content behind a COPA-compliant screen.

2. Plaintiff Joan Walsh
   Salon Media Group, Inc.
   101 Spear Street, Suite 203
   San Francisco, CA 94105

Ms. Walsh is the editor of the online magazine Salon.com. She will testify to the nature of Salon's Web site and the sexual content of some of the speech on that site. She will testify that Salon fears prosecution under COPA for that speech and will explain the reasons for that fear. She will testify that there are other speakers on the Web who engage in similar speech, some of whom may be beyond the reach of COPA. She will testify that Salon could not operate its Web site with its existing content according to its best editorial and business judgment if Salon had to place all of the sexual content behind a COPA-compliant screen.

3. Expert witness: Dr. Lorrie Faith Cranor
   Department Of Computer Science
   Carnegie Mellon University
   5000 Forbes Avenue
   Pittsburgh, PA 15213

Dr. Cranor is an Associate Research Professor in the School of Computer Science at Carnegie Mellon University. She has been qualified as an expert in Internet content filtering technology and issues relating to speech on the Internet in several previous federal cases. Further details about her expert qualifications are contained in her resume, a copy of which is attached hereto.

Dr. Cranor will testify that Internet content filters are widely and freely available and can be used easily and effectively to limit access to materials communicated via the Internet that may be deemed harmful to minors. She will further testify that such filters can block material or services regardless of its geographical origins, whether it is published for a commercial or non-commercial purpose, whether it is free or requires payment, and regardless of whether it is distributed over the World Wide Web or the other regularly used parts of the Internet. She will further testify that filtering products provide parents with the means to supervise and control the Internet activities of their children. Dr. Cranor will testify that filters are therefore a far more effective, flexible and less restrictive alternative to COPA. She will further testify that there are a variety of non-filtering-based tools such as education and parental involvement that provide additional less restrictive, yet effective, means of limiting access to online materials that parents may not want their children to access.

4. Ms. Rebecca Caroline Gilbert
U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington, DC 20530-0001

Ms. Gilbert is an employee of Defendant responsible for the Internet content filters used by the Department of Justice. Ms. Gilbert will testify that she and Defendant are satisfied with the degree of protection and effectiveness provided by the filters used by the Defendant.

5. DOJ Witness re Definitions in COPA
U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington, DC 20530-0001

Plaintiffs will seek to subpoena Defendant or his designee to testify to Defendant's interpretation, policies, guidelines or rationales concerning COPA, and to apply those interpretations, policies, guidelines or rationales.

6. Expert Witness: Professor Henry Reichman
Department of History
Cal State East Bay
25800 Carlos Bee Blvd.
Hayward, CA 94542-3045

Professor Reichman is a Professor of History at California State University, East Bay, and Associate Editor of the American Library Association's "Newsletter on Intellectual Freedom." He is also author of *Censorship and Selection: Issues and Answers for Schools*. Further details about his expert qualifications are contained in his resume, a copy of which is attached hereto.

Professor Reichman will testify to efforts that have been made across the United States to censor or prosecute speech about sex in the name of protecting children from harm. He will testify that the speech that has been the subject of such efforts has been similar to, but in many cases more innocent than, the speech that Plaintiffs present on their Web sites.

7. Expert Witness: Mr. Michael Russo
2925-B Gulf Freeway South
PMB # 111
League City, Texas 77573

Mr. Russo is President of YNOT Network, LP, a company that provides useful information and services to adult entertainment professionals and hobbyists including the online adult industry. He has been associated with the adult industry since 1992. He has operated adult

Web sites, and has used credit card and other possible age verification systems in connection with his Web sites. Since 2000, he has been editor in chief of TheAdultWebmaster.com, a trade publication for the online adult content industry. In that connection, he has studied the use of various online payment card screens and other data verification systems, attended conferences that included discussion of such systems, and published articles on such systems. Further details about his expert qualifications are contained in his resume, a copy of which is attached hereto.

Mr. Russo will testify that payment card verification systems are flawed and easy to bypass, that payment card associations prohibit use of payment cards as a proxy for age, and that setting up and use of a payment card verification system costs money. Mr. Russo will also testify that services that verify data other than payment card information ("Data Verification Services") suffer from additional shortcomings, including geographical limitations and limitations on feedback regarding unauthorized use, and that they too are not effective for use by online content providers to verify the age of Web site visitors. He will further testify that all such systems will impose significant financial costs on Web sites. Mr. Russo will also testify that a significant amount of adult material is provided by overseas sites, on non-commercial sites, and through Internet technologies (such as peer-to-peer) file sharing networks other than the World Wide Web. Mr. Russo will further testify that implementation of COPA will lead to the relocation of adult online content providers outside the United States and the reduced attendance of web sites that place content behind payment card or data verification screens.

8. Expert Witness: Dr. Matthew Zook
   University of Kentucky
   Department of Geography
   1457 Patterson Office Tower
   Lexington, KY 40506

Dr. Zook is a Professor of Geography at the University of Kentucky. He has published widely on the use and geographical diffusion of the Internet and the domain name system. He has published more specifically on the geography of the Internet adult industry, including the location of content production, Web sites, and hosting. Further details about his expert qualifications are contained in his resume, a copy of which is attached hereto.

Dr. Zook will testify that less than fifty percent of free adult Web sites are located in the United States and that this share has steadily declined since 2001.

9. Plaintiff Adam Glickman
647 Poinsetia Place
Los Angeles, CA 90036

Mr. Glickman is the operator of an online store and Web site called Condomania.com. He will testify to the nature of his Web site and the sexual content of the speech. He will testify that he fears prosecution under COPA for that speech and will explain the reasons for that fear. He will testify that there are other speakers on the Web who engage in similar speech, some of whom may be beyond the reach of COPA. He will testify that he could not operate his Web site if he had to place all of the content behind a COPA-compliant screen.

10. Ms. Alicia Smith
Brooklyn, NY

Ms. Smith is a lesbian hip-hop musician who works under the name God-Des. Her work is available on the World Wide Web, including on her own Web site. She will testify to the nature of her Web speech and the sexual content of the speech. She will testify that she fears prosecution under COPA for that speech and will explain the reasons for that fear. She will testify that there are other speakers on the Web who engage in similar speech, some of whom may be beyond the reach of COPA.

11. Plaintiff Mitchell Tepper
3 Mayflower Lane
Shelton, CT 06484

Mr. Tepper is the operator of the Web site, Sexual Health Network.com, which provides easy and free access to information about sexuality and sexual health, particularly for individuals with disabilities. He will testify to the nature of his Web site and the sexual content of the speech. He will testify that he fears prosecution under COPA for that speech and will explain the reasons for that fear. He will testify that there are other speakers on the Web who engage in similar speech, some of whom may be beyond the reach of COPA. He will testify that he could not operate his Web site if he had to place the content behind a COPA-compliant screen.

12. Expert Witness: Professor Ronald Mann
The University of Texas Law School
727 E. Dean Keeton Street
Austin, TX 78705

Professor Mann is a law professor who specializes in the study of electronic commerce and payment systems with a particular emphasis on credit cards. He holds the Ben H. & Kitty King Powell Chair in Business and Commercial Law at the University of Texas School of Law and is Co-Director and Founder of the Center for Law, Business, and Economics. Further details about his expert qualifications are contained in his resume, a copy of which is attached hereto.

Professor Mann will testify that far more than fifty percent of all children have access to payment cards while they are minors, and that the estimates of Defendant's expert, Arthur Clark, are not reliable and fail to weigh adequately the aggressive marketing of payment cards to minors, the increasing prevalence of prepaid cards among minors, and the reality of unauthorized and unsupervised payment card use by minors. He will also testify that payment card companies will not enforce COPA overseas for the federal government because doing so would require them to take the unprecedented step of first making a unilateral assessment of which overseas

sites fail to comply with COPA and of then voiding perfectly legal transactions (e.g., the sale of non-obscene material to adults) based on that assessment. Finally, he will rebut criticisms made by Mr. Clark of the COPA Commission's findings that payment cards are not an effective or reliable means of verifying age.

13. Expert Witness: Dr. Edward W. Felten
Dept. of Computer Science
Princeton University
35 Olden Street
Princeton, NJ 08544

Dr. Felten is a Professor of Computer Science and Public Affairs at Princeton University and Director of Princeton's Center for Information Technology and Policy. Dr. Felten has been qualified as an expert in diverse fields related to computer science in several prior federal cases. Further details about his expert qualifications are contained in his resume, a copy of which is attached hereto.

Dr. Felten will testify that various forms of online speech, including email, peer-to-peer distribution, streaming audio and video, instant messaging and chat, voice over IP, ftp, and television over the Internet, will not be covered by COPA because they are not transmitted "by means of the World Wide Web" under the language of COPA. Dr. Felten will testify that significant amounts of speech are transmitted by those means. Dr. Felten will also testify that Web sites seeking to evade COPA's requirements can do so easily and successfully by distributing their material using the ftp protocol rather than the http protocol. Dr. Felten will further testify that there are no technological impediments to applying Internet content filtering to speech accessed through new Internet access devices such as cell phones, iPods, PDAs, and game consoles. Dr. Felten will testify that numerous vendors currently have sophisticated content filtering products for use on these alternative devices, and that some mobile carriers are

already offering parental controls to their users. Dr. Felten will also testify about search engines and, specifically, that because of the way search engines work: (1) age verification screens would prevent Web pages from being seen because they cannot be indexed; (2) it is less likely than in the past that individuals will accidentally encounter unwanted content; and (3) it is more accurate to think of one Web page as a "whole," rather than to think of the entirety of a Web site as a whole. Dr. Felten will also testify that few minors have the technical expertise to circumvent Internet Content filters, and that there are no unique installation or usability problems associated with Internet filtering software that are not common to all software.

14. Plaintiff Aaron Peckham
1600 Amphitheater Parkway, 41-220C
Mountain View, CA 94043

Mr. Peckham is the operator of an online slang dictionary called UrbanDictionary.com. He will testify to the nature of his Web site and the sexual content of the speech. He will testify that he fears prosecution under COPA for that speech and will explain the reasons for that fear. He will testify that there are other speakers on the Web who engage in similar speech, some of whom may be beyond the reach of COPA. He will testify that he could not operate his Web site if he had to place the content behind a COPA-compliant screen.

15. Mr. Wayne Snellen
26 Wooster Street
New York, NY 10013

Mr. Snellen is an artist and the Director of the Leslie/Lohman Gay Art Foundation. He will testify to the nature of his art and the art on the Foundation's Web site, and the sexual content of the art. He will testify that he fears prosecution under COPA for that speech and will explain the reasons for that fear. He will testify that there are other speakers on the Web who

engage in similar speech, some of whom may be beyond the reach of COPA. He will testify that he could not operate his web site if he had to place the content behind a COPA-compliant screen.

16. Ms. Marilyn Jaye Lewis
205 S. Hamilton Rd.
Gahanna OH 43230-2969

Ms. Lewis is founder and Director of the Erotic Author's Association. She will testify to the nature of the Association's Web site and the sexual content of the speech. She will testify that she and other members within the association fear prosecution under COPA for their speech and will explain the reasons for that fear. She will testify that there are other speakers on the Web who engage in similar speech, some of whom may be beyond the reach of COPA. She will testify that the Association could not operate its Web site if it had to place the content behind a COPA-compliant screen.

17. Mr. Joseph Fried
505 Thornall Street, Suite 305
Edison, New Jersey 08837

Mr. Joseph Fried is an employee of Flash Networks, a company that provides solutions to mobile carriers wishing to improve the experience their customers have when using data services, such as Internet access. He will testify that his company provides technology that can be used to filter content on mobile devices such as cell phones, and that his company has entered into an agreement to provide its filtering technology to a mobile carrier in the United States. Mr. Fried will also testify about the other companies in the industry that provide similar filtering technology for mobile Internet access devices.

18. Mr. Dwight Wesley Miller
P.O. Box 615
Pilot Point, TX, 76258

Mr. Miller is the owner of an art gallery in Pilot Point, Texas. For more than two years, he was publicly threatened with prosecution by law enforcement for a mural on the outside of the wall of his gallery that was allegedly harmful to minors. He will testify about the nature of the mural and the governmental efforts concerning the mural.

19. Ms. Terri Kirk
Reidland High School
5349 Benton Road
Paducah, KY 42003

Ms. Kirk is a librarian at the Reidland High School in Paducah, Kentucky. Her school district utilizes an Internet content filter on its student computers, and supervises and educates students on the use of the Internet. She will testify that the district is satisfied with the protection provided to its students through these means.

20. Ms. Clover Taylor
Western Albemarle High School
5941 Rockfish Gap Turnpike
Crozet, VA 22932

Ms. Taylor is a librarian at the Western Albemarle High School in Crozet, Virginia, a suburb of Charlottesville. Her school district utilizes an Internet content filter on its student computers, and supervises and educates students on the use of the Internet. She will testify that the district is satisfied with the protection provided to its students through these means.

21. Ms. Tava Smathers
Telluride Schools
725 West Colorado Avenue
Telluride, CO 81435

Ms. Smathers is a librarian at the Telluride Schools in Telluride, Colorado. Her school district utilizes an Internet content filter on its student computers, and supervises and educates students on the use of the Internet. She will testify that the district is satisfied with the protection provided to its students through these means.

22. Mr. Jonjie Sena
ACE*COMM Corporation
704 Quince Orchard Road, Suite 100
Gaithersburg, Maryland USA 20878

Mr. Sena is Director of Product Management of Ace*Comm, a company that provides business intelligence and advanced operations support systems solutions to telecommunications service providers. He will testify that his company provides technology that can be used to filter content on mobile devices such as cell phones, and that his company's technology is currently being deployed by a mobile carrier in North America. Mr. Sena will also testify about the other companies in the industry that provide similar filtering technology for mobile Internet access devices.

23. Ms. Barbara DeGenevieve
School of the Art Institute of Chicago
Photography Department
Care of Barbara DeGenevieve
280 South Columbus Ave
Chicago, IL 60603

Ms. DeGenevieve is a professor at the School of the Art Institute of Chicago. She is also an interdisciplinary artist, photographer and video maker. Her work is available on the Web. She will testify to the nature of her work and the sexual content of that work. She will testify that she fears prosecution under COPA for that speech and will explain the reasons for that fear. She will testify that there are other speakers on the Web who engage in similar speech, some of whom may be beyond the reach of COPA.

24. Plaintiff Heather Corrine Rearick
Washington State

Ms. Rearick is the operator of three online Web sites, scarleteen.com, scarletletters.com and femmerotic.com. She will testify to the nature of her Web sites and the sexual content of the speech. She will testify that she fears prosecution under COPA for that speech and will explain

the reasons for that fear. She will testify that there are other speakers on the Web who engage in similar speech, some of whom may be beyond the reach of COPA. She will testify that she could not operate the Scarleteen site, which is designed for minors, if she had to place its content behind a COPA-compliant screen. She will testify that she could not operate her other sites with their existing content according to her best editorial and business judgment if she had to place all of the sexual content behind a COPA-compliant screen.

In addition, if the Court does not permit use of any of the deposition designations listed in Section IX below, Plaintiffs will seek to call each of those individuals as witnesses.

25. Rebuttal Expert Witness: Dr. Andrew Gelman
Department of Statistics
Columbia University
1255 Amsterdam Ave., 10th Floor
New York, NY 10027

Dr. Gelman is a tenured professor in the Departments of Statistics and Political Science at Columbia University. Further details about his expert qualifications are contained in his resume, a copy of which is attached hereto.

If the statistical testimony of Defendant's expert Jeffrey Eisenach is permitted, Dr. Gelman will testify that Mr. Eisenach's methodology is unsupportable, and that, based on the data cited by Mr. Eisenach, the most reliable estimate of the rate of use of filtering software among Internet-using households with children in the United States is 54%.

26. Rebuttal Expert Witness: Mr. J. Christopher Racich
First Advantage Litigation Consulting
14030 Thunderbolt Place, Suite 700
Chantilly, VA 20151

Mr. Racich is Vice President and Counsel for First Advantage, a computer forensics company located in Chantilly, Virginia. Further details about his expert qualifications are contained in his resume, a copy of which is attached hereto.

If the testimony of Defendant's expert Paul Mewett is permitted, Mr. Racich will testify that using Web pages classified by Mr. Mewett, he tested two additional Internet content filters not tested by Mr. Mewett. He will testify that SafeEyes's product had a blocking success rate of 87.27% and that 8e6's product had a blocking success rate of 90.23%.

B. Defendant's witnesses

1. Ernie Allen
President and CEO
National Center for Missing &
Exploited Children
699 Prince Street
Alexandria, VA 22314

Summary of Fact Witness Testimony: Mr. Allen is expected to testify to the problem of minors' unwanted exposure to sexually explicit content on the Internet. He is expected to testify that in 1999, his organization, the National Center for Missing & Exploited Children, commissioned the Crimes Against Children Research Center to conduct the Online Victimization of Youth study, and that in 2005, it commissioned the second Online Victimization of Youth study to measure changes in the problem since the first study.

2. David Finkelhor
Professor of Sociology
Director, Crimes against Children Research Center
Co-Director, Family Research Laboratory
University of New Hampshire
Durham, NH 03824

Summary of Fact Witness Testimony: Dr. Finkelhor is expected to testify to the factual results contained in the August 9, 2006, *Online Victimization of Youth: Five Years Later* report, of which he is the principal and supervisory author. Specifically, with respect to 10-17 year-old's unwanted exposure to sexually explicit material on the Internet at home, and the efficacy of filtering software on the families' home computers, he is expected to testify to the factual results of the underlying 2005 survey, and is expected to contrast those results with those from a similar survey he headed five years earlier.

3. Dr. Stephen Neale
Department of Philosophy
Rutgers University
New Brunswick, NJ 08901

Summary of Expert Testimony:

Dr. Stephen Neale is an expert in linguistics, mathematical logic, cognitive science, and the philosophy of language. Dr. Neale is expected to testify regarding issues in the field of linguistics relating to the efficacy of Internet content filtering software. His testimony will include evaluation of linguistic, logical, and conceptual issues involved in text filtering, the heart of contemporary Internet filtering.

Dr. Neale will offer the opinion that content filtering technology alone (or in conjunction with other currently available methods) does not provide a particularly effective means of ensuring that minors under 17 are not exposed to sexually explicit content available on commercial websites, and it will not do so in the foreseeable future.

Summary of Expert Qualifications:

Since 1999, Dr. Neale has been a Professor of Philosophy at Rutgers University, where he holds the rank of Professor II, a special designation within the rank of (Full) Professor. His area of expertise is what is usually called the philosophy of language, which includes the study of syntax, semantics, logical analysis, formal systems, computability theory, context, translation and interpretation, all of which he has worked on extensively. He is an affiliated member of the Department of Linguistics at Rutgers and the Center for Cognitive Science. He has been a Guggenheim fellow, a Rockefeller fellow, a fellow of the National Endowment for the Humanities (NEH), and a President's Fellow of the University of California. He has published widely in peer review journals and other refereed academic publications, and he has lectured around the world over the past twenty years, as an invited speaker at both academic institutions and professional conferences in philosophy, linguistics, mathematical logic, and computer science. He was a professor at the University of California, Berkeley from 1990 to 1998, where he was tenured in 1993 and promoted to Full Professor in 1998. At Berkeley, he was a member of the Graduate Program in Logic and Methodology of Science, which he chaired for several years. He was an Assistant Professor of Philosophy and Linguistics at Princeton University from 1988 to 1990 and a member of the Program in Cognitive Science. He received his Ph.D. from Stanford University in 1988. He began his doctoral work in the Ph.D. program in linguistics in the Department of Linguistics and Philosophy at MIT in 1983, moved to the PhD program in linguistics at Stanford in 1984, and obtained the PhD in the field of philosophy in 1988 with a dissertation bridging linguistic semantics and the philosophy of language.

4. Paul Mewett
CRA International
1 Undershaft
London EC3A 8EE
United Kingdom

Summary of Expert Testimony:

Mr. Mewett will testify with regard to the structure, architecture, and size of the World Wide Web, and with regard to the functions of internet content filtering software programs. He will testify with regard to the technological limitations of those programs. He will further testify with regard to the results of a study that he and Dr. Stark performed of sexually explicit material

on the World Wide Web, and regarding the significance of those results. In particular, Dr. Stark will testify regarding the prevalence of sexually explicit websites on the Web, the proportion of those websites that are domestically hosted or that have commercial ties to the United States, and the effectiveness of internet content filtering software products at blocking sexually explicit websites, and at avoiding the blocking of non-sexually explicit websites.

Mr. Mewett will also present rebuttal testimony regarding: (1) the claims of plaintiffs' proffered expert witness, Lorrie Faith Cranor, concerning the effectiveness of filtering software programs; (2) the claims of plaintiffs' proffered expert witness, Edward Felten, regarding the use of the FTP protocol for internet communications; and (3) the claims of plaintiffs' proffered expert witness, Matthew Zook, regarding the prevalence of non-commercial sexually explicit websites, or of sexually explicit websites located outside of the United States. Mr. Mewett will also present sur-rebuttal testimony, if needed, concerning the underblocking and overblocking rates of internet content filtering products tested by plaintiffs' proffered rebuttal expert witness, J. Christopher Racich.

Summary of Expert Qualifications:

Mr. Mewett is qualified to testify as an expert with regard to technical aspects of the operations of computers and of the Internet and the World Wide Web. He is a Principal in the London office of CRA International. He is the head of the Internet Intelligence Unit, which supports both CRA's Forensic Investigations Practice and it Computer Forensics Practice. As the head of the Internet Intelligence Unit, he uses his skills and knowledge relating to mining the Internet and other electronic media to support the investigations of the Forensic Investigations Practice and the Computer Forensics Practice. Over the last ten years, all of his major projects have involved the Internet. For the past 25 years, his specialty has been in assisting organizations to evaluate and implement new technologies.

Over the last four years, he has worked with law enforcement in North America and in the United Kingdom, as well as the National Center for Missing and Exploited Children, where he has managed the technical challenges relating to tracking and identifying child pornography on the Internet. He has also run programs to track credit card fraud and identity theft which takes place in the Deep Web. These programs require him to apply his comprehensive knowledge of the Internet, its architecture, and the technical innovations that have enabled the Internet's rapid expansion. He has performed analysis for a number of clients that involved gathering of data sets and drawing conclusions from the data that was collected. As one example, he recently performed a study for a mobile telecommunications client that involved identifying locations on the Internet that were sharing intellectual property, and that also involved analyzing those Websites to determine if the operators of those Websites could be located.

Before joining CRA International, he founded and took public a company that focused on the retrieval of information from the Internet for large companies. He was instrumental in the design and development of the spider technology, as well as the business strategy, that made the company a success. That spider technology was created specifically to be able to "crawl" around the Surface Web and to identify information specific to a company's name or brand. His clients

for this technology included a number of global banks, a major German automotive company, a pharmaceutical company, and a major global health care company. He has also held the post of Chief Technical Officer for another company, ASP Solutions Ltd., in the field of Internet Intelligence Solutions. The company used "best of breed" and in-house tools to identify and deliver business intelligence from the Surface Web and the Deep Web for major branded clients. He served as an electronics engineer for the British Ministry of Defense, and received electronics qualifications from the School of Royal Electrical and Mechanical Engineers for the Ministry of Defense in 1984.

5. Philip B. Stark, Ph.D.
University of California, Berkeley
403 Evans Hall
Berkeley, CA 94720

Summary of Expert Testimony:

Dr. Stark will testify regarding the results of a statistical study that he and Paul Mewett performed of sexually explicit material on the World Wide Web, and regarding the significance of those results. In particular, Dr. Stark will testify regarding the prevalence of sexually explicit websites on the Web, the proportion of those websites that are domestically hosted or that have commercial ties to the United States, and the effectiveness of internet content filtering software products at blocking sexually explicit websites, and at avoiding the blocking of non-sexually explicit websites. He will also present rebuttal testimony regarding the methodology of plaintiffs' proffered expert witnesses, Matthew Zook and Lorrie Faith Cranor. He will also present sur-rebuttal testimony, if needed, concerning the underblocking and overblocking rates of internet content filtering products tested by plaintiffs' proffered rebuttal expert witness, J. Christopher Racich.

Summary of Expert Qualifications:

Philip Stark is qualified to testify as an expert with regard to the application of statistical techniques to the Internet. He is a Professor of Statistics at the University of California, Berkeley. He has been on the Statistics faculty at that university since 1988. He has been a Miller Research Professor, a Dodson Fellow, a Presidential Chair Fellow, and a Mellon/Library Faculty Fellow. He received a Bachelor's degree from Princeton University in 1980 and a Ph.D. from the University of California, San Diego, in 1986. He was a Presidential Young Investigator and a National Science Foundation Postdoctoral Fellow in Mathematical Sciences. He is a member of the American Geophysical Union, the Bernoulli Society for Mathematical Statistics and Probability, the Center for Astrostatistics, the Center for Data Analysis Technology and Applications, the Global Oscillation Network Group, the Institute of Physics, the Institute of Mathematical Statistics, the National Partnership for Advanced Computational Infrastructure, the Royal Astronomical Society, the Solar and Heliospheric Observatory Solar Oscillations Investigation, the Space Sciences Laboratory, and the Theoretical Astrophysics Center. He has been on the editorial board of several journals, and has written over 65 articles and technical reports. He has given approximately 130 invited lectures at scientific conference and universities in 16 countries. He has testified before the U.S. House of Representatives' Subcommittee on the

Census and the California Senate's Natural Resources Committee. He has consulted for the U.S. Department of Justice, the Federal Trade Commission, the U.S. Department of Agriculture, the U.S. Census Bureau, the U.S. Attorney's Office for the Northern District of California, the U.S. Department of Veterans Affairs, the Los Angeles County Superior Court, the National Solar Observatory, public utilities, major corporations, and numerous law firms. He has testified as an expert witness, or has served as a non-testifying expert, in cases involving antitrust, consumer class actions, employment discrimination, equal protection, fairness in lending, federal legislation, insurance, intellectual property, product liability, trade secrets, truth in advertising, and wage and hour disputes. Some of his consulting and research relates to the Internet, including characterizing and predicting online consumer behavior and developing search algorithms. He created a web-based statistics course using HTML, JavaScript and Java, the most widely used web languages. He has been on the advisory boards of a web marketing firm and two online publishers.

6. Jeffrey A. Eisenach, Ph.D.
Chairman
Criterion Economics
1620 I Street, N.W.
Washington, D.C. 20006

Summary of Expert Testimony:

Dr. Eisenach, who is an expert on the Internet and its impact on markets and public policy, is expected to testify, *inter alia*, that Internet content filtering ("ICF") software is the only software that allows children to access the Internet while not having access to inappropriate material. The potential market for home-based ICF software is the approximately 41 percent of Internet-connected households with children. Market survey evidence suggests that approximately four out of these ten Internet-connected households with children use ICF software. This percentage indicates a failure of the market to provide products which are effective and can be effectively used by consumers.

A significant proportion of households that do not use ICF software are deterred from using it, or have tried to use it and stopped, because they find the available products to be too complex, too ineffective, or a combination of the two. The costs of using ICF software include the time parents must spend installing, setting up and maintaining the software, which for many parents, are a significant deterrent to ICF software use, and for some, an insurmountable one. ICF products are more difficult to install than word processing products, and are more difficult to use than other types of software.

ICF software causes over blocking and under blocking, and can be circumvented by children. Parents, accordingly, are deterred from using ICF software. There is a demand for good ICF products that is not being met. The nature of ICF software and market therefore are conducive to market failure because of the asymmetry of information between consumers and producers of the ICF software. The market for ICF software is smaller than the market for other kinds of security software, thereby causing ICF software producers to have weaker incentives to improve the quality of their product, and contributing to market failure.

Summary of Expert Qualifications:

Dr. Eisenach is an expert on the Internet and its impact on markets and public policy. He has performed studies on the use of Microsoft's Internet Explorer and Operating Systems software, as well as of the use of peer-to-peer software. Dr. Eisenach is the Chairman of Criterion Economics, LLC, an economic and financial consulting firm based in Washington, D.C. Prior to joining Criterion Economics, LLC in 2006, he was Chairman of CapAnalysis, LLC, an economic and financial consulting firm based in Washington, D.C.

Dr. Eisenach received a Ph.D. in economics from the University of Virginia in May 1985, and has taught economics and/or public policy at the Kennedy School of Government at Harvard University, George Mason University Law School, the University of Virginia, and Virginia Polytechnic Institute and State University. Prior to joining CapAnalysis in 2003, Dr. Eisenach served for 10 years as President of the Progress & Freedom Foundation, a research organization that studies the Internet and its implications for public policy. While in that position, he authored or co-authored more than two dozen research papers and submissions to regulatory agencies on the Internet and communications issues, including an annual volume called the Digital Economy Fact Book, which is a compilation of economic data relating to the Internet, communications technologies and software. Dr. Eisenach has co-edited scholarly books on antitrust issues in the market for computer operating systems and applications, and on the role of government regulation of telecommunications markets.

7. Douglas Knopper
President and CEO
Bitpass
4600 Bohannon Drive
Suite 100A
Menlo Park, CA 94025

Summary of Fact Witness Testimony: Mr. Knopper will testify about Bitpass and its iMedia Commerce Engine, a digital wallet application that offers consumers single-click, micro-payment purchasing of online content and complete privacy and anonymity. Mr. Knopper will testify about how the product works from the perspective of merchants and consumers, as well as about various features that are underdevelopment or consideration, including a version of the product availabel to merchants that accepts only Bitpass accounts tied to a payment card, a modification of the product that allows parents to monitor their children's Bitpass activity, and consideration of a feature that would allow consumers to "purchase" content for free by watching a video advertisement.

8. Dr. Scott M. Smith
1361 Lakeview Drive
Provo, Utah 84604

Summary of Expert Testimony:

Dr. Smith will testify about the effect of COPA on commercial websites on the Internet. He will testify about the growth of Internet commerce and the increasing willingness of consumers to provide personal information on the Internet. He will testify that barriers are common in successful everyday shopping activities on the Internet, and that COPA's regulation of access to certain content by minors under the age of 17 will have no significant adverse effect on adults who access, search for information, or use the Internet.

Dr. Smith will also testify about consumers' willingness to tolerate economic barriers in the form of time, inconvenience, or money to achieve a goal. He will note that the pornography industry traditionally has faced both social and technological barriers that have not reduced industry demand and that every time a new medium for the dissemination of pornography has been created, the technological advances have required not only a shift in consumer use behavior, but a shift in the business model within the industry.

Summary of Expert Qualifications:

Scott M. Smith, Ph.D., is the James M. Passey Professor of Marketing and Director of the Institute for Marketing in the Marriot School of Management, Brigham Young University. Dr. Smith is an expert in (1) Internet research and methodology; (2) advanced computer applications for Internet survey research and analysis; (3) cross-cultural research; (4) consumer behavior; and (5) Internet business models. He has co-authored a textbook on the fundamentals of market research, and has authored or co-authored twelve books or monographs and more than 60 articles or papers, including a book on Internet marketing. He has worked as a research consultant for IBM, Microsoft, and Yahoo!

Dr. Smith is the Founder and Director of Qualtrics, Inc., SurveyZ.com, and SurveyPro.com. These online Applications offer the most advanced survey research, database, and analysis tools available and are used by companies like the U.S. Army, The Conference Board, Celebrity Cruises, Intel, Kodak, Micron, Yahoo!, Microsoft, Travelocity, ATI, Sabre Holdings, Royal Caribbean, and Motorola.

Dr. Smith is the co-author of the textbook *Fundamentals of Marketing Research* (Sage Publications, 2005) and the PC-MDS statistical software programs for multidimensional statistical analysis. He authored or co-authored 12 books and monographs and more than 60 articles and papers. He has published in *Marketing Research, Journal of Marketing Research, Journal of Consumer Research, Journal of Business Research, Journal of the Academy of Marketing Science, Journal of Marketing Education* (awarded the year's outstanding article), and *Journal of Business Ethics*. The academic books also include, *Multidimensional Scaling, Computer Assisted Decisions in Marketing*, and *Internet Marketing*.

Dr. Smith has served on the editorial board of Health Marketing Quarterly, Journal of Health Care Marketing and has reviewed for Journal of Marketing Research, and the Journal of the Academy of Marketing Science. He is the past president of the Association for Health Care Research.

Dr. Smith has instructed executive courses in research methodology for IBM Corporation and the American Marketing Association Professional Division and has been an active research consultant for the following companies: IBM, Microsoft, Yahoo!, ATI, Iomega, Bell South, Caterpillar, Johnson and Johnson, Miles Labs, Nissan, Novell, Pioneer-Hi-bred Seed Company, Quaker, Sarah Lee, Staples, Simplot, and the U.S. Army. Dr. Smith currently teaches "Marketing Research," "Measurement and Analysis," and "Field Studies" courses in the undergraduate and MBA programs at BYU. His earned degrees are from Brigham Young University (B.S. Business, 1971), Michigan State (MBA, 1973), and Pennsylvania State University (Ph.D., 1979). Dr. Smith wrote his dissertation on segmenting retail shoppers.

9. Arthur E. Clark, Jr.
Business Insights Consulting, Inc.
11 South Highland Street
Nyack, NY 10960

Summary of Expert Testimony:

Arthur E. Clark, Jr. is an expert in payment cards. Mr. Clark is expected to testify about the effectiveness of restricting, in good faith, access by minors to material that is harmful to minors by requiring the use of a credit card or debit account, including testimony that:

(1) Credit, debit and prepaid cards, known as payment cards, are popular and easy to use. The vast majority of adult U.S. consumers have made purchases on line with a payment card.

(2) Most adults own either a credit card or a debit card tied to their checking account. Even "unbanked" adults can acquire and use reloadable prepaid cards to make purchases on the Web. Pursuant to the requirements of the "Know Your Customer" provisions of the USA Patriot Act, issuing banks require a purchaser of a reloadable prepaid card to be an adult.

(3) Almost no children under 12 and a very small minority of teens ages 12-16 have a payment card consisting of either an "extra" card on their parent's account or a "parent co-signed" card in the child's name. A very small minority of teens occasionally borrow their parents cards to make purchases. Age of majority laws prevent card issuers from issuing payment cards to children in their own name.

(4) Parents can supervise their children's online transactions at the time of purchase. But even if actual purchases made with these cards are unsupervised, parents can see their children's payment card purchases online soon after the purchase is made, and, in some cases, the same day. Virtually all adult cardholders are familiar with reviewing a billing statement, and with calling the card issuer to inquire about unfamiliar or suspect purchases.

(5) The emergence of (non-reloadable) prepaid gift cards is not an obstacle to limiting children's access to harmful to minors material. Non-reloadable gift cards do not have a billing address and present a higher degree fraud risk Web merchants that can not successfully perform the two operational verifications now common for most online transactions (*i.e.*, billing address and CVC), are likely to decline that transaction. Indeed, the two primary Internet Payment

Service Providers that control the adult entertainment market require a billing address in order to purchase access to online adult entertainment.

(6) Requiring the use of a payment card before website visitors can access adult sexual content on these websites places almost no burden on these merchants. The costs to honor the traditional payment cards are modest and even lower for PayPal. These costs, fraud and processing fees, are likely to decline over the next three to five years.

(7) Requiring the use of a payment card to view adult sexual content "monetizes" a product that is in high demand. Although requiring the use of a payment card may reduce the number of website visitors, such visitors were unlikely to make a purchase, and thus unlikely to affect business results.

(8) Each of the payment card companies have worldwide policies, operating rules and agreements, which govern any retailer or website operator worldwide that accepts payment cards. These agreements require compliance with all applicable laws and regulations. Merchant agreements even require foreign merchants selling goods and services to U.S. customers to comply with U.S. laws. Thus, once COPA is in effect, foreign commercial adult sexual content providers will have to require use of a payment card before a visitor can view adult sexual content on their websites or risk fines or rescission of their right to accept cards.

(9) Non-profit business and law enforcement communities recently announced the organization of the Financial Coalition Against Child Pornography. The Coalition set up a CyberTipline to identify website operators that sell child pornography, cut off their use of payment cards, and share this information with law enforcement communities. By identifying website operators that do not restrict access to adult sexual content, cutting off their use of payment cards, and sharing this information with law enforcement communities, the payment industry and law enforcement target international commercial websites just as easily as domestic ones. Adapting the Financial Coalition Against Child Pornography to include COPA would essentially be a "fine tuning" process to focus also on commercial website operators that provide adult sexual content. The net result would be that children's access to adult sexual content (adult sex acts and content) would be targeted for world-wide control and enforcement.

In addition, Mr. Clark will offer sur-rebuttal testimony to each of the three proffered opinions of Prof. Ronald J. Mann offered in his expert rebuttal report.

Summary of Expert Qualifications:

Mr. Clark has thirty-five years of industry experience that includes both management positions at American Express, Citigroup, Dow Jones, and management consulting. Mr. Clark has experience in the use of payment cards on the Internet developed from doing consulting projects for Amazon, NetCharge, and American Express. Mr. Clark also has experience with assisting banks in developing prepaid cards for the youth market. In addition, Mr. Clark has experience with assisting acquiring banks in signing up new merchants and with assisting banks in developing secured payment cards for unbanked persons. Mr. Clark has served as expert witness relating to payment cards in four other cases.

Mr. Clark has significant experience in reading research results from both his corporate experience and his consulting experience, including working with research departments in designing studies to meet business needs, so that the data from the study is projectable and usable for business purposes. He has had a great deal of influence on whether survey research is conducted over the phone, in person, or in focus groups in both quantitative and qualitative research, and has played a significant role in determining the sample sizes of the survey research. Industry research and consumer research is at the core of Mr. Clark's ability to do his job. His firm is constantly assembling proprietary data on rates of fraudulent and/or unauthorized uses of payment cards and rates of adoption and/or use of payment cards across various segments of the population in different types of sales transactions.

Mr. Clark has experience in marketing prepaid cards to the youth market from a project he did and is doing for First Financial Bank, which focuses on the youth market. Mr. Clark is an expert in payment cards, including, among other things, what payment cards are used for on the Internet by consumers and merchants, how they work, the adoption rates, fraud rates, and the amount of payments per transaction.

10. Marie Alexander
President and CEO
Quova
707 California Street
Mountain View, CA 94041

Summary of Fact Witness Testimony: Ms. Allen will testify about Quova and its Internet geolocation service, which allows Internet providers to ascertain the location of individuals with whom they do business. Ms. Alexander's testimony will include a description of the geolocation services product, its common usage in business and by government, and its accuracy.

11. Gary Connor
Director of Research, Quova
707 California Street
Mountain View, CA 94041

Summary of Fact Witness Testimony: Mr. Connor will testify about Quova's Internet geolocation service, which allows Internet providers to ascertain the location of individuals with whom they do business. Mr. Connor's testimony will include the process by which the geolocation services product works.

12. Pattie Suozzi Dillon
President, Veratad Technologies, LLC
155 N. Dean Street
Englewood, NJ 07631

Summary of Fact Witness Testimony: Ms. Dillon will testify about ID Response, an online age verification service. During fact discovery, Defendant identified ID Response as an age

verification service that could be used to establish an affirmative defense under COPA. Ms. Dillon will testify regarding Veratad=s current products and products in development that can be used to verify age online.

13. John Dancu
President and CEO, IDology, Inc.
One Overton Park
3625 Cumberland Blvd., Suite 350
Atlanta, GA 30339

Summary of Fact Witness Testimony: Mr. Dancu will testify about IDology, an online age verification service. During fact discovery, Defendant identified IDology as an age verification service that could be used to establish an affirmative defense under COPA. Mr. Dancu will testify regarding IDology=s current products and products in development that can be used to verify age online.

14. Philip Scott
Paralegal, U.S. Department of Justice
20 Massachusetts Avenue, NW
Washington, DC 20530

Summary of Testimony: Mr. Scott will authenticate, if necessary, certain documents proffered by Defendant as exhibits.

15. Tim Sloane
Director, Credit & Advisory Service
Mercator Advisory Group, Inc.
1432 Main Street
Waltham, MA 02451

Summary of Fact Witness Testimony: Mr. Sloane will offer sur-rebuttal testimony in response to the proposed testimony of Professor Ronald Mann concerning prepaid cards, including their development, market share, and regulation.

VI. Exhibits

A. Plaintiffs' Exhibits

1. Resume of Lorrie Faith Cranor

2. Expert report of Lorrie Faith Cranor; Cranor Rebuttal report

3. DOJ e-Testing Labs study, October 2001; DOJ e-Testing Labs study, March 2002

4. DOJ Finnell report, October 15, 2001; DOJ Finnell Rebuttal report, November 30,

2001.

5. NetAlert study, 2001
6. COPA Commission report, October 2000
7. Munroe, Cybersitter 9.0 review, Aug. 3, 2004, PC Magazine
8. Consumer Reports, "Filtering Software: Better But still Fallible," June 2005
9. Auld, Hampton, "Filters Work," American Libraries, Feb. 1, 2003
10. Lenhart, Pew Internet and American Life Project, "Protecting Teens Online," PEW, March 2005
11. Department of Commerce, Children's Internet Protection Act, Aug. 2003
12. Resume of Edward W. Felten
13. Expert report of Edward W. Felten; Felten Rebuttal report
14. Pew Internet & American Life Project, *Generations Online* (Dec. 2005).
15. Pew Internet & American Life Project, *Search Engine Use* (Nov. 2005)
16. Pew Internet & American Life Project, *Teen Content Creators and Consumers* (Nov. 2005).
17. Pew Internet & American Life Project, *Teens and Technology, Youth Are Leading the Transition to a Fully Wired and Mobile Nation*, (July 2005).
18. Edward W. Felten's Web page in HTTP, at http://cs.princeton.edu/~felten
19. Illustration of conversion of Edward W. Felten's Web page to FTP, resulting in ftp://ftp.cs.princeton.edu/pub/people/felten/index.html.
20. Alltel *Axcess Web*, at http://www.alltel.com/axcess/mobile_web.html
21. Resume of Henry Reichman

22. Expert report of Henry Reichman
23. Newsletters on Intellectual Freedom, Jan. 2004-March, 2006
24. Resume of Michael Russo
25. Expert report of Michael Russo
26. Testimony of Mark McCarthy, Visa USA before the Commission on Online Protection
27. GAO Report to Congressional Requesters: File Sharing Programs, The Use of Peer-to-Peer Networks to Access Pornography, 2005
28. Resume of Matthew Zook
29. Expert report of Matthew Zook
30. Zook tables 1-9
31. Zook figures 1-3
32. Zook, M. *Underground globalization*, Environment and Planning, Vol. 35(7), 1261-1286.
33. Resume of Ronald Mann
34. Expert rebuttal report of Ronald Mann
35. Resume of Andrew Gelman
36. Expert rebuttal report of Andrew Gelman
37. Select pages from Web site of Plaintiff Sexual Health Network
38. Select pages from Web site of Plaintiff Nerve
39. Select pages from Web site of Plaintiff Salon
40. Select pages from Web site of Plaintiff Condomania
41. Select pages from Web site of Plaintiff Aaron Peckham

42. Select pages from Web sites of Plaintiff Heather Corrine Rearick

43. Select pages from Web site of Plaintiff ACLU members Ferlinghetti and Warren

44. Select pages from Web site of Plaintiff Free Speech Media.

45. Select pages from Web site of Plaintiff Philadelphia Gay News

46. Select pages from Web site of Plaintiff Powell's Bookstores.

47. Photos of Wes Miller's mural

48. Letters to Wes Miller from Pilot Point Police

49. Select pages from Web site of Leslie/Lohman Gallery Web site

50. Lyrics of songs by God-des

51. CD of songs by God-des

52. Select pages from Web site of Erotic Authors Association

53. DVD of select pages of work of Barbara DeGenevieve

54. NRC Report, 2002

55. October 1998 letter from DOJ to Rep. Bliley

56. March 9, 2000 testimony of DOJ to Subcommittee on Crime, Committee of the Judiciary, US House of Representatives

57. Urban Dictionary Editor Guidelines

58. Cisco Systems, *Cisco Mobile Exchange Solution Overview, at* http://www.cisco.rw/en/US/netsol/ns341/ns396/ns177/ns278/networking_solutions_white_paper09186a008012a9f9.shtml

59. Cisco Systems, *Mobile Content Filtering and Control: Why it is Needed, How it Works, at*

http://www.cisco.rw/en/US/netsol/ns341/ns396/ns177/ns278/networking_solutions_white_paper0900aecd8025e7f9.shtml.

60. Blue Coat, *News Releases, at* http://www.bluecoat.com/news/releases/2006/041006-mobile.html.

61. Bytemobile, *Bytemobile ACCESS Mobile Content Filtering, at* http://www.bytemobile.com/products/accessmobile.html

62. Boston Consulting Group, Inc., *Mobile Guardian, at* http://www.bcgi.net/pdf/presskit/bcgi_MobGuard.pdf

63. *Alltel Offers Parents a More Family-Friendly Mobile Web* (March 30, 2006), *at* *http://www.alltel.com/corporate/media/news/06/march/n411march3006a.html*

64. Firefly, *User Guide for Parents, at* https://onlinecare.cingular.com/devicehelp/FireflyUserManual.pdf).

65. Letter, Bruce Taylor to Rev. Kirk, September 10, 2002 [Bates D-1 S 002362]

66. List of obscenity cases filed by Defendant, September 4, 2001-November 1, 2002 [Bates D-1 B002430-33]

67. Master List: Obscenity Cases and Investigations updated as of May 23, 2003 [Bates D-1 B 002434-38]

68. A Brief Look at the Work of the Child Exploitation and Obscenity Section, April 19, 2005 [Bates D-1 B,C 002676]

69. Letter, DOJ Criminal Division to Geraldine Corey, March 21, 2002 [Bates D-6 S 000666-67.

70. ACE*COMM, “Illustrations of ParentPatrol user interface”
71. CCBill E-Ticket Flow Demo (same as Cadwell Deposition Exhibit 3, in color, printed on 10/03/06)
72. CCBill ISO Agreement (Cadwell Deposition Exhibit 8)
73. CCBill Acceptable Use Policies (Cadwell Deposition Exhibit 10)
74. Epoch Systems – Adult Entertainment Website Compliance
75. IDresponse Application for Services
76. IDresponse – Rules of the Data
77. Affidavit of J. Blair Richardson
78. IDliveAge Quick Start Guide (Dancu Deposition Exhibit 3)
79. Web Portal End User Tips: Age and Identity Verification (Dancu Deposition Exhibit 6)
80. Idology Document entitled “MSA Part 4; Schedule A” (Dancu Deposition Exhibit 9)
81. United States Law Week article – “Young Hackers for Hire by Criminals Turn to Carding, Counterfeit IDs to Pay Rent” (Feb. 28, 2006)
82. Palisade Systems, “Peer-to-Peer Study Results” Executive Summary, 2003
83. Second CD by God-Des
84. AOL Document, bates-numbered AOL 551
85. AOL Study, bates-numbered AOL 1880-81
86. Powerpoint Demonstration of AOL Parental Controls
87. Select pages from Getnetwise.org
88. Toptenreviews 2006 Internet Filter Report

89. Microsoft Document, “Parental Controls in Windows Vista,” bates-numbered MS 004074-4090

90. Teenage Research Unlimited: Study Methodology [Mann Dep. Exh. 3]

91. Junior Achievement Worldwide: Personal Finance, 2006 [Mann Dep. Exh. 6]

92. Teenage Research Unlimited: Survey Questionnaire [Mann Dep. Exh. 9

93. Teenage Research Unlimited: Response Data [Mann Dep. Exh. 10]

94. All Access Prepaid Card [Mann Dep. Exh. 10A]

95. All Access Prepaid Card FAQ [Mann Dep. Exh. 11]

96. All Access Terms and Conditions [Mann Dep. Exh. 13]

97. Internetretailer.com, “A Majority of U.S. Online Teens Have Shopped on the Web, Forrester Says” [Mann Dep. Exh. 16]

98. Jolayne Houtz, “Look Who’s Whipping Out the Credit Card, High Schoolers,” Seattle Times [Mann Dep. Exh. 16]

99. Lori Hawkins, “Netspending: Prepaid Card Combines Online Services, Ease of Debit for Bank-Wary Consumers,” Austin American-Stateman [Mann Dep. Exh. 19]

100. “Babies Receiving Credit Card Applications,” DenverChannel.com article [Mann Dep. Exh. 20]

101. Ronald J. Mann and Seth R. Belzey, “The Promise of Internet Intermediary Liability,” [Mann Dep. Exh. 24]

102. Diagram of Typical AVS Transaction (Russo Report)

103. Diagram of Typical Paysite Transaction (Russo Report)

104. Diagram of Typical DVS Transaction (Russo Report)

105. CCBill Transaction Processing Agreement (Cadwell Deposition Exhibit 9)

106. Universal Services Agreement (Thaler Deposition Exhibit 1)

107. New High-Risk Internet Service Provider Program Introduced (Thaler Deposition Exhibit 5)

108. Federal Trade Commission Staff Report – "Peer-to-Peer File Sharing Technology: Consumer Protection and Competition Issues" (June 2005)

109. Testimony Before the United States Senate Committee on the Judiciary – "Pornography, Technology and Process: Problems and Solutions on Peer-to-Peer Networks" by Dr. Doug Jacobson

110. Select Webpages from Download.com

111. Select Peer-to-Peer Application Video Files

112. Select Peer-to-Peer Application Image Files

113. Select Peer-to-Peer Application Screen Shots

114. Select UseNet Application Screen Shots

115. Select Google Search Screen Shots

116. Select Email Application Screen Shots

117. Select UseNet Application Image Files

118. Select pages from Web site of Plaintiff EFF member Bill Boushka

119. Samples of non-COPA means of communication

120. Resume of Christopher Racich.

121. Expert Supplemental Report of Christopher Racich.

If the Court does not permit use of the deposition designations and exhibits listed in Section IX below, those exhibits should be included on Plaintiffs' list of trial exhibits.

B. Defendant's exhibits

D 1	A Report on the Nation's Youth by the Crimes Against Children Research Center, David Finkelhor, Kimberly J. Mitchell, Janis Wolak dated June 2000
D 2	Online Victimization of Youth: Five Years Later by the Crimes Against Children Research Center, Janis Wolak, Kimberly Mitchell, David Finkelhor dated 2006
D 3	Curriculum Vitae of David Finkelhor
D 4	Expert Report of Jeffrey A. Eisenach, Ph.D. dated May 8, 2006
D 5	Rebuttal Report of Jeffrey A. Eisenach, Ph.D. dated July 6, 2006
D 6	Curriculum Vitae of Jeffrey A. Eisenach, Ph.D.
D 7	AOL Parental Controls, Control Access to Browsers and Other Internet Programs on This Computer: Off
D 8	The Digital Future Report, Survey the Digital Future, Year Four, Ten Years, Ten Trends dated September 2004
D 9	U.S. Census Bureau, Computer and Internet Use in the United States: 2003 dated October 2005
D 10	Center for the Digital Future, USC Annenberg School dated December 7, 2005
D 11	Article - Cities find Wi-Fi Future by Amy Cox dated October 18, 2004
D 12	Article - Commentary: Getting Home Networking Into Second Gear by Forrester Research dated January 27, 2005
D 13	High-Speed Services for Internet Access: Status as of June 30, 2005, Industry Analysis and Technology Division, Wireline Competition Bureau dated April 2006
D 14	Article - Kids Outsmart Web Filters by Stefanie Olsen dated April 19, 2006
D 15	McAfee Parental Controls Reviewer's Comments
D 16	AOL/NCSA Online Safety Study Conducted by America Online and the National Cyber Security Alliance dated October 2004
D 17	A Nation Online: How Americans Are Expanding Their Use of The Internet by the U.S. Department of Commerce dated February 2002
D 18	A Nation Online: Entering The Broadband Age by the U.S. Department of Commerce dated September 2004
D 19	NetGear, 108 Mbps Wireless Firewall Router
D 20	NetGear, Reference Manual for the 108 Mbps Wireless Firewall Router WGT624 v3 dated April 2005
D 21	Article - U.S. Broadband Connections Reach Critical Mass, Crossing 50 Percent Mark for Web Surfers, According to Nielsen/Netratings dated August 18, 2004

D 22	Article - Two-Thirds of Active U.S. Web Population Using Broadband, Up 28 Percent Year-Over-Year to an All-Time High, According to Nielsen/Netratings dated March 14, 2006
D 23	Article - Two Out of Every Five Americans Have Broadband Access at Home, According to Nielsen/Netratings dated September 28, 2005
D 24	Kids Ages 2-11 Lead Growth in Web Page Consumption, According to Nielsen/Netratings dated November 17, 2004
D 25	Norton Parental Controls Review's Comments dated 2006
D 26	Sony PlayStation Portable, Instructional Manual, PSP 1001
D 27	Article - Router-Based Parental Controls by Nick Stam dated August 3, 2004
D 28	Open Forum On Decency Before the Committee on Commerce, Science, and Transportation United States Senate, 109th Cong., 1st Sess. , dated November 29, 2005
D 29	The Market for "Lemons": Quality Uncertainty and the Market Mechanism by George A. Akerlof dated August 1970
D 30	Article - Cellphone Technology Rings in Pornography in USA by Gary Strauss dated December 12, 2005
D 31	Wireless Philadelphia, Executive Committee, Briefing
D 32	Premiums for High Quality Products as Returns to Reputations by Carl Shapiro
D 33	The UCLA Internet Report, Surveying the Digital Future, Year Three dated February 2003
D 34	The Role of Market Forces in Assuring Contractual Performance by Benjamin Klein and Keith B. Leffler
D 35	Quacks, Lemons, and Licensing: A Theory of Minimum Quality Standards by Hayne E. Leland
D 36	Information and Consumer Behavior by Phillip Nelson
D 37	Advertising as Information by Phillip Nelson
D 38	Letter from Michael W. Quinn, Time Warner Cable to Joel McElvain, Department of Justice dated October 6, 2005
D 39	PCMag.Com, Child-Proofing Windows
D 40	PCMagazine 2004 Enterprise Product Summary, Content- Filtering Software and Hardware
D 41	Websense Administrator's Guide
D 42	IDC Analyze the Future, Broadband Services Evolution - Moving Beyond the Pipe

D 43	Websense Installation Guide, Stand-Alone Edition
D 44	Horizontal Merger Guidelines by the Department of Justice and Federal Trade Commission issued April 2, 1992, revised April 8, 1997
D 45	Third Annual Open Prepaid Markey Survey: Spend, Growth, and Opportunity dated August 2006
D 46	AOL - Total Base After Adjusting
D 47	Symantec Home Networking
D 48	Websense Web Security Suite Quick Start Guide
D 49	MSN - Key Findings Overall
D 50	MSN - Problems Using Internet Software
D 51	MSN - Performance on NB ISP
D 52	Bell South Flow Chart
D 53	Verizon Five Year Forecast
D 54	SurfControl User Guides For All Products
D 55	SurfControl Web Filter 5.0, Administrator's Guide
D 56	CyberPatrol, User Guide
D 57	CyberPatrol, Quick Start Guide
D 58	AOL Report Summary, At Home With Moms and Kids dated February 17, 2005
D 59	Expert Report of Stephen Neale corrected July 3, 2006
D 60	Curriculum Vitae Stephen Neale
D 61	Expert Report of Geoffrey Nunberg (redacted)
D 62	Expert Report of Philip B. Stark, Ph.D. dated May 8, 2006
D 63	Rebuttal Expert Report of Philip B. Stark, Ph.D. dated July 6, 2006
D 64	Curriculum Vitae of Philip B. Stark
D 65	Table - Prevalence of Sexually Explicit Webpages
D 66	Table - Confidence Limits for the Prevalence of Sexually Explicit Webpages
D 67	Table - Underblocking and Overblocking of Webpages in Search Indexes (redacted)
D 68	Table - Underblocking and Overblocking of Webpages in Search Indexes

D 69	Table - Confidence Limits for Underblocking and Overblocking of Webpages in Search Indexes (redacted)
D 70	Table - Confidence Limits for Underblocking and Overblocking of Webpages in Search Indexes
D 71	Table - Percentage of Domestic Webpages Among Underblocked Webpages in Search Indexes (redacted)
D 72	Table - Percentage of Domestic Webpages Among Underblocked Webpages in Search Indexes
D 73	Table - Underblocking and Overblocking for AOL, MSN and Yahoo! Queries (redacted)
D 74	Table - Underblocking and Overblocking for AOL, MSN and Yahoo! Queries
D 75	Table - Confidence Limits for Underblocking of AOL, MSN and Yahoo! Queries (redacted)
D 76	Table - Confidence Limits for Underblocking of AOL, MSN and Yahoo! Queries
D 77	Table - Underblocking and Overblocking for Wordtracker Queries (redacted)
D 78	Table - Underblocking and Overblocking for Wordtracker Queries
D 79	Table - Foreign “Free” Webpages with Commercial Ties to the U.S.
D 80	BetonSports Indictment
D 81	Institute of Education Sciences, National Center for Education Statistics, Computer and Internet Use by Students in 2003, Statistical Analysis Report dated September 2006
D 82	Expert Report of Paul Mewett dated May 8, 2006
D 83	Rebuttal Expert Report of Paul Mewett dated July 6, 2006
D 84	Curriculum Vitae Paul Mewett
D 85	Chart of Plaintiffs’ Websites That Were Blocked by Filters
D 86	Set of Web Pages Depicting Use of Google Cache
D 87	Set of Web Pages Depicting Use of Google Translation
D 88	Sexually Explicit Web Pages from Mewett Study (pp. 1-40/42?)
D 89	Print-out from Webpage www.cexx.org
D 90	Print-out from Webpage www.zensur.freerk.com
D 91	Expert Report of Scott M. Smith, Ph.D. dated May 8, 2006
D 92	Curriculum Vitae Scott M. Smith, Ph.D.

D 93	Expert Report Arthur E. Clark dated May 8, 2006
D 94	Curriculum Vitae Arthur E. Clark
D 95	Figure 1.2.1 from Expert Report of Clark
D 96	Figure 2.3.1 from Expert Report of Clark
D 97	Figure 2.3.3 from Expert Report of Clark
D 98	Figure 3.2.1 from Expert Report of Clark
D 99	Figure 3.3.1 from Expert Report of Clark
D 100	Figure 3.5.1 from Expert Report of Clark
D 101	Figure 3.6.1 from Expert Report of Clark
D 102	Figure 3.8.3 from Expert Report of Clark
D 103	Figure 4.3.1 from Expert Report of Clark
D 104	Figure D.1 from Expert Report of Clark
D 105	Excerpt from Expert Report of Clark ,Appendix E: Age of Majority Law Review
D 106	Excerpt from Expert Report of Clark quoting “traditional payment card has five unique characteristics”
D 107	DOJ Overview - Introduction to Bitpass dated August 29, 2006
D 108	Veratad Age and Identity Verification Processing through IDResponse Privacy Platform Products
D 109	IDology - Overview of Age Verification Product
D 110	Sexual Health Network - Main Page
D 111	About Us - Our Mission
D 112	Experts - Sexual Health Editorial Team
D 113	Sexual Health Network - Membership Page
D 114	Sexual Health Network - Store
D 115	Store - Second Party Credit Card Page
D 116	Sexual Health - Video Library
D 117	Men’s Sexual Health Section
D 118	Women’s Sexual Health Section
D 119	Sexuality Education Section

D 120	German Shepherd - Questions and Answers by Mitchell Tepper
D 121	Mentally Challenged Masturbation Video - Questions and Answers
D 122	Article - Sexual Pleasure - But What About Me? By Mitch Tepper dated May 4, 2004
D 123	Article - The Joys That Vibrators Can Bring to Your Sex Life dated May 4, 2004
D 124	Article - 20 Helpful Hints for Women to Reach Orgasm by Cynthia Lief Ruberg
D 125	Nerve Teaser Opening Page
D 126	Nerve - Main Page
D 127	Nerve - About Us
D 128	Nerve - About Our Business
D 129	Mission Statement - What Are We Thinking
D 130	Nerve Partners
D 131	Shop - Products
D 132	Premium Subscription Page
D 133	Premium Package Page - Credit Card Information
D 134	Premium Subscription - Free Tour
D 135	Fiction Section
D 136	Henry Miller Award October 2005
D 137	San Francisco Noir by Peter Maravelis
D 138	Photography Section
D 139	Red Light Specters by Sylvia Plachy (Photo 1)
D 140	The Blue Danube by Sylvia Plachy (Photo 2)
D 141	Tableaux Vivants by Bettina Rheims
D 142	Blogs Section
D 143	Blog-A-Log
D 144	Salon Teaser Opening Page
D 145	Teaser Ad Page
D 146	Salon - Main Page
D 147	Salon - Directory

D 148	Salon - Fact Sheet
D 149	Salon's Mission
D 150	Get the Full Salon Experience - Membership Subscription Page
D 151	Billing and Shipping - Store - Second Party Credit Card Page
D 152	Community Forums and Blogs
D 153	Index - Gay
D 154	Index - Homosexuality
D 155	Index - Lesbians
D 156	Index - Oral Sex
D 157	Index - Sex
D 158	Index - Sexuality
D 159	Article - Aroused My First Porn Movie by Susie Bright
D 160	Article - Go Out and Get a Piece, Son! by Lara Riscol dated May 21, 2002
D 161	Article - Mike Bloomberg's Coming-Out Story by Lynn Harris dated January 12, 2005
D 162	Article - Rectal Romance by Rebecca Traister dated October 8, 2004
D 163	Article - Rome's Latest Witch Hunt Won't Stop With Gays by Sara Miles dated October 3, 2005
D 164	Article - South Korean Women Can't Get no Satisfaction by Page Rockwell dated February 10, 2006
D 165	Article - The Virginity Hoax by Jennifer Foote Sweeney
D 166	Article - We are "Natural Family" by Lynn Harris dated January 25, 2006
D 167	Article - You Pussy by Margot Magowan dated February 28, 2001
D 168	Condomania's Main Page
D 169	About Us - Welcome to the Land of Latex, Condomania
D 170	Here's All The Details About Ordering at Condomania
D 171	Order - Credit Card Page - Payment Options
D 172	Affiliate Program - Make Some Cash Fast
D 173	Condom Blog - Condoms, Sex, & Desire
D 174	Safer Sex Manual - Getting Educated at Condomania

D 175	Condoms Section
D 176	Gifts & Novelties
D 177	Condomania's Road Test - Reviews From All Over
D 178	Femmerotic Teaser Opening Page
D 179	Heather Corinna - Main Page
D 180	About Heather Corinna
D 181	Journal
D 182	Journal Frequently Asked Questions
D 183	The Long and the Short of Biography
D 184	You Can Take it With You - Membership Subscription
D 185	Join TicketsClub - Membership Subscription's Second Party Site
D 186	Stories Without Words (Photography and Art) Section
D 187	Scarlet Letters Teaser Opening Page
D 188	Scarlet Letters - Main Page
D 189	About Scarlet
D 190	Membership Subscription Page
D 191	Join TicketsClub - Membership Subscription's Second Party Site
D 192	Scarlet Letters Interactive - Message Boards
D 193	Nonfiction Section
D 194	Prose & Poetry Section
D 195	Visual Art Section
D 196	Scarleteen - Main Page
D 197	Scarleteen - Site Map
D 198	About Scarleteen and Our Staff
D 199	Help Scarleteen With Your Donation
D 200	How to Shop Here
D 201	Shop's Second Party Site
D 202	Condom Basics a Users Manual - A Simple Condom Primer

D 203	A Date Rape Drug - A Special Report
D 204	Orgasm and Sexual Response Article
D 205	Sound Off - Message Board Guidelines
D 206	Sound Off - Message Board
D 207	Boyfriend Section - Main Page
D 208	Boyfriend Section - Advice
D 209	Boyfriend Section - Articles
D 210	Gaydar Section - Main Page
D 211	Gaydar Section - Advice
D 212	Gaydar Section - Articles
D 213	Pink Slip Section - Main Page
D 214	Pink Slip Section - Advice
D 215	Pink Slip Section - Articles
D 216	Reproduction Section - Main Page
D 217	Reproduction Section- Advice
D 218	Reproduction Section - Articles
D 219	Sexual Politics Section - Main Page
D 220	Sexual Politics Section - Advice
D 221	Sexual Politics Section - Articles
D 222	Sexyouality Section - Main Page
D 223	Sexyouality Section - Advice
D 224	Sexyouality Section - Articles
D 225	Skin Deep Section - Main Page
D 226	Skin Deep Section - Advice
D 227	Skin Deep Section - Articles
D 228	Take Two Section - Main Page
D 229	Take Two Section - Advice
D 230	Take Two Section - Articles

D 231	Infection Section - More Infection Section - Main Page
D 232	Infection Section - Advice
D 233	Infection Section - Articles
D 234	Urban Dictionary - Main Page
D 235	Bearded Claim (definition)
D 236	Blumpkin (definition)
D 237	Booty (definition)
D 238	Chode (definition)
D 239	Cleveland Steamer (definition)
D 240	Cock (definition)
D 241	Cornhole (definition)
D 242	Dirty Sanchez (definition)
D 243	Donkey Punch (definition)
D 244	Dripping Delta (definition)
D 245	Frottage (definition)
D 246	Fuck (definition)
D 247	Pearl Necklace (definition)
D 248	Santorum (definition)
D 249	Smegma (definition)
D 250	Stench Trench (definition)
D 251	Taint (definition)
D 252	Teabagging (definition)
D 253	Experiences of High School Students Conducting Term Paper Research Using Filtered Internet Access by Lynn Sorensen Sutton dated 2005
D 254	Technology & Science, Filtering Porn? Maybe, Maybe Not by Bobbi Nodell dated August 9, 2000
D 255	Consumer Report 2001, Digital Chaperones for Kids
D 256	Report eTesting Labs
D 257	Article - Does Pornography-Blocking Software Block Access to Health Information on the Internet?

D 258	A Kaiser Family Foundation Study, See No Evil: How Internet Filters Affect the Search for Online Health Information dated December 2002
D 259	Internet Filters a Public Policy Report by Marjorie Heins and Christina Cho dated 2001
D 260	A Study on Internet Access in Educational Institutions, Internet Blocking in Public Schools, Version 1.1 of 26 dated June 2003
D 261	Newsletter on Intellectual Freedom by Judith F. King dated May 2006
D 262	Partnership Agreement between Idology Group and Ynot Network dated July 21, 2005
D 263	Hecker Excerpt - 100 Adult Porn
D 264	Hecker Excerpt - Adult-XXX BBS
D 265	Hecker Excerpt - Exotic Porn Show
D 266	Hecker Excerpt - Free Porn Movies
D 267	Hecker Excerpt - Gaypiczone
D 268	Hecker Excerpt - Hardcore Studio
D 269	Hecker Excerpt - Nikki's Last Stand
D 270	Hecker Excerpt - Quickporn
D 271	Hecker Excerpt - Takeitoff
D 272	Hecker Excerpt - Tools
D 273	Hecker Excerpt - XXX Fantasy
D 274	Testimony of Professor James B. Weaver, III, U.S. Senate Committee on Commerce, Science & Transportation, Hearing on "Protecting Children on Internet" dated January 19, 2006
D 275	Exhibit A to Contention Interrogatories
D 276	Exhibit B to Contention Interrogatories
D 277	Exhibit to Contention Interrogatory 4
D 278	Exhibit to Contention Interrogatory 5
D 279	Defendant's Supplemental Response to Plaintiffs' Initial Interrogatories dated January 27, 2006
D 280	Defendant's Supplemental Response to Plaintiffs' Initial Interrogatories dated March 13, 2006
D 281	Defendant's Supplemental Response to Plaintiff's Initial Interrogatories dated March 16, 2006

D 282	Defendant's Supplemental Response to Plaintiffs' First Set of Contention Interrogatories dated August 14, 2006
D 283	Defendant's Second Supplemental Response to Plaintiffs' First Set of Contention Interrogatories dated September 27, 2006
D 284	Letter from Eric Beane, Department of Justice to Honorable Lowell A. Reed, Jr. dated September 5, 2006
D 285	Bill Boushka's Responses and Objections to Defendant's First Set of Interrogatories
D 286	Condomania's Responses and Objections to Defendant's First Set of Interrogatories
D 287	Ferlinghetti's Responses and Objections to Defendant's First Set of Interrogatories
D 288	Free Speech Media LLC Public Communications Inc. Responses and Objections to Defendant's First Set of Interrogatories
D 289	Nerve's Responses and Objections to Defendant's First Set of Interrogatories
D 290	Aaron Peckham d/b/a Urban Dictionary.com's Responses and Objections to Defendant's First Set of Interrogatories
D 291	Philadelphia Gay News Responses and Objections to Defendant's First Set of Interrogatories
D 292	Powell's Books Responses and Objections to Defendant's First Set of Interrogatories
D 293	Rearick's Responses and Objections to Defendant's First Set of Interrogatories
D 294	Salon Media Group Inc. Responses and Objections to Defendant's First Set of Interrogatories
D 295	Sexual Health Network Responses and Objections to Defendant's First Set of Interrogatories
D 296	Patricia Nell Warren's Responses and Objections to Defendant's First Set of Interrogatories
D 297	Bill Boushka's Responses and Objections to Defendant's Second Set of Interrogatories
D 298	Condomania's Responses and Objections to Defendant's Second Set of Interrogatories
D 299	Ferlinghetti's Responses and Objections to Defendant's Second Set of Interrogatories
D 300	Free Speech Media LLC Public Communications Inc. Responses and Objections to Defendant's Second Set of Interrogatories
D 301	Nerve's Responses and Objections to Defendant's Second Set of Interrogatories
D 302	Aaron Peckham d/b/a Urban Dictionary.com's Responses and Objections to Defendant's Second Set of Interrogatories

D 303	Philadelphia Gay News Responses and Objections to Defendant's Second Set of Interrogatories
D 304	Powell's Books Responses and Objections to Defendant's Second Set of Interrogatories
D 305	Rearick's Responses and Objections to Defendant's Second Set of Interrogatories
D 306	Salon Media Group Inc. Responses and Objections to Defendant's Second Set of Interrogatories
D 307	Sexual Health Network Responses and Objections to Defendant's Second Set of Interrogatories
D 308	Patricia Nell Warren's Responses and Objections to Defendant's Second Set of Interrogatories
D 309	eMarketer, North America Online: Demographics & Usage dated February 2003
D 310	Article from Website, Sexuality Information and Education, Sex and Meaning dated February 14, 2006 (Tepper Exh. 1)
D 311	Excerpt from Website, Sexual Health, dated February 9, 2006 (Tepper Exh. 3)
D 312	Article from Website, Sexuality Information and Education, Men's Sexual Health dated February 14, 2006 (Tepper Exh. 4)
D 313	Article from Website, Sexuality Information and Education, Sexual Pleasure: But What About Me? by Mitch Tepper dated May 4, 2004 (Tepper Exh. 5)
D 314	Excerpt from Website, Sexuality Information and Education, Question and Answer, Reviewed by Mitch Tepper dated May 6, 2004 (Tepper Exh. 6)
D 315	Excerpt from Sexual Health Network Website, Sexuality Information and Education, Information about the Sexual Editorial Team dated February 14, 2006 (Tepper Exh. 7)
D 316	Sexual Health Network, Inc.'s Responses and Objections to Defendant's First Set of Interrogatories dated October 28, 2005 (Tepper Exh. 8)
D 317	Nerve Media (Bates 86-113) (Nerve Depo Exh. A)
D 318	Summary of Nerve Media (Nerve Depo Exh. B)
D 319	Page from Website entitled About Us - Partners (Nerve Depo Exh. C)
D 320	Page from Website entitled About Us - Business, Editors, Design, Technology (Nerve Depo Exh. D)
D 321	Pages from Website - Premium Subscription and Free Tour (Nerve Depo Exh. E)
D 322	The Courting of Anatomy by Helen Walsh (Nerve Depo Exh. F)
D 323	Mystery Tour by Luke Sutherland (Nerve Depo Exh. G)

D 324	The Henry Miller Award (Nerve Depo Exh. H)
D 325	First page of the Blog-A-Log section (Nerve Depo Exh. I)
D 326	Article from Website - You Pussy by Margot Magowan dated February 28, 2001 (Salon Depo Exh. A)
D 327	Article from Website - Aroused My First Porn Movie dated March 18, 1997 (Salon Depo Exh. B)
D 328	Article from Website - Rectal Romance by Rebecca Traister dated October 8, 2004 (Salon Depo Exh. C)
D 329	List of articles under the category of Sex dated January 4, 2006 (Salon Depo Exh. D)
D 330	Article from Broadsheet - South Korean Women Can't Get no Satisfaction by Page Rockwell dated February 10, 2006 (Salon Depo Exh. E)
D 331	List of articles under the category of Sexuality dated January 4, 2006 (Salon Depo Exh. F)
D 332	Article - Go Out and Get a Piece, Son! by Lara Riscol dated May 21, 2002 (Salon Depo Exh. G)
D 333	List of articles under the category of Homosexuality dated January 4, 2006 (Salon Depo Exh. H)
D 334	Article from Website - Rome's Latest Witch Hunt Won't Stop With Gays by Sara Miles dated October 3, 2005 (Salon Depo Exh. I)
D 335	List of articles under the category of Gay dated January 4, 2006 (Salon Depo Exh. J)
D 336	Article from Broadsheet - We are "Natural Family" by Lynn Harris dated January 25, 2006 (Salon Depo Exh. K)
D 337	List of articles under the category of Lesbians dated January 4, 2006 (Salon Depo Exh. L)
D 338	Article from Broadsheet - Mike Bloomberg's Coming-Out Story by Lynn Harris dated January 12, 2005 (Salon Depo Exh. M)
D 339	List of articles under the category of Oral Sex dated January 4, 2006 (Salon Depo Exh. N)
D 340	Article - The Virginity Hoax by Jennifer Foote Sweeney (Salon Depo Exh. O)
D 341	Scarleteen - About Our Staff (Rearick Depo Exh. 1)
D 342	Excerpt from Website - Sexual Response Questions and Answers (Rearick Depo Exh. 2)
D 343	Story - Date Rape Drugs, A Special Report (Rearick Depo Exh. 3)

D 344	Story - The Making of a Homo by James Elliott (Rearick Depo Exh. 4)
D 345	Excerpt from Website - Infection Section Articles (Rearick Depo Exh. 5)
D 346	Teaser Opening Page for Scarlet Letters (Rearick Depo Exh. 6)
D 347	Main Page for Scarlet Letters (Rearick Depo Exh. 7)
D 348	Excerpt from Website - About the Scarlet Letters Website (Rearick Depo Exh. 8)
D 349	Teaser Opening Page for Femmerotic Website (Rearick Depo Exh. 9)
D 350	Main Page for Femmerotic Website (Rearick Depo Exh. 10)
D 351	Article - You Can Take it With You (Rearick Depo Exh. 11)
D 352	Article - Stories Without Words Photograph (Rearick Depo Exh. 12)
D 353	Excerpt from eTesting Labs, Corporate Content Filtering Performance and Effectiveness Testing dated March 2002 (Cranor Depo Exh. 4)
D 354	Report - Effectiveness of Internet Filtering Software Products Prepared for NetAlter and the Australian Broadcasting Authority by Paul Greenfield, Peter Rickwood, Huu Cuong Tran dated September 2001 (Cranor Depo Exh. 6)
D 355	A Review - PC Magazine, Cybersitter 9.0 by Jay Munro dated August 3, 2004 (Cranor Depo Exh. 7)
D 356	Story - ConsumerReports, Filtering Software: Better, But Still Fallible (Cranor Depo Exh. 8)
D 357	Report - American Library Association, Filters Work: Get Over It dated February 1, 2003, Vol. 34, Issue 2 (Cranor Depo Exh. 9)
D 358	Curriculum Vitae of Henry F. Reichman dated July 2005 (Reichman Depo Exh. 1)
D 359	The Extent of the Problem (Reichman Depo Exh. 3)
D 360	Banned and Challenged Books in Texas Schools (March 2005)(Reichman Depo Exh. 4)
D 361	“Dirty” Words (Reichman Depo Exh. 5)
D 362	Red Carpet Ratings Services (January 2004) (Reichman Depo Exh. 6)
D 363	Article from Newsletter on Intellectual Freedom, pp. 11-12 (January 2004) (Reichman Depo Exh. 7)
D 364	Article from Newsletter on Intellectual Freedom, p. 56 (Reichman Depo Exh. 8)
D 365	Article from Newsletter on Intellectual Freedom, p. 9 (January 2004) (Reichman Depo Exh. 9)

D 366	Article from Newsletter on Intellectual Freedom, p. 231 (November 2004) (Reichman Depo Exh. 10)
D 367	Article from Newsletter on Intellectual Freedom, p. 50 (Reichman Depo Exh. 11)
D 368	Article from Newsletter on Intellectual Freedom, p. 13 (January 2002) (Reichman Depo Exh. 12)
D 369	Article from Newsletter on Intellectual Freedom, pp. 19-20 (January 2005) (Reichman Depo Exh. 13)
D 370	Article from Newsletter on Intellectual Freedom, pp. 155-156 (July 2005) (Reichman Depo Exh. 14)
D 371	Article from Newsletter on Intellectual Freedom, pp. 145-146 (July 2001) (Reichman Depo Exh. 15)
D 372	Article from Newsletter on Intellectual Freedom, p. 197 (September 2002) (Reichman Depo Exh. 16)
D 373	Article from Newsletter on Intellectual Freedom, pp. 50-51 (March 2004) (Reichman Depo Exh. 17)
D 374	Article from Newsletter on Intellectual Freedom, p. 10 (Reichman Depo Exh. 18)
D 375	Article from Newsletter on Intellectual Freedom, pp. 156-157 (July 2005) (Reichman Depo Exh. 19)
D 376	Article from Newsletter on Intellectual Freedom, pp. 158-159 (July 2005) (Reichman Depo Exh. 20)
D 377	Article from Newsletter on Intellectual Freedom, p. 7 (January 2004) (Reichman Depo Exh. 21)
D 378	Article from Newsletter on Intellectual Freedom, pp. 34 (Reichman Depo Exh. 22)
D 379	Texas Lawyer, Vol. 21, No. 40, All About Eve - Settlement Allows Outdoor Display of Nude Painting by Mark Donald dated December 5, 2005 (Reichman Depo Exh. 23)
D 380	The Detroit News, Nudity in Mural Divides Residents by George Hunter dated February 27, 2005 (Reichman Depo Exh. 24)
D 381	Free Speech Coalition, Brief History of XXX (Russo Depo Exh. 2)
D 382	Free Speech Coalition, Draft Code of Ethics and Best Practices dated July 7, 2006 (Russo Depo Exh. 3)
D 383	Visa Buxx, Frequently Asked Questions (Russo Depo Exh. 4)
D 384	Article - Illegal Transactions May Not Be Submitted Into The Visa Payment System by Michael E. Smith (Russo Depo Exh. 5)
D 385	Outline of Discussion Areas (Russo Depo Exh. 6)

D 386	Print-outs of Web Pages Not Blocked by SafeEyes (Racich Depo Exh. L)
D 387	Print-outs of Web Pages Not Blocked by 8e6 (Racich Depo Exh. M)
D 388	Expert Report of Matthew A. Zook (Zook Depo Exh. 1)
D 389	Environmental and Planning A 2003, Vol. 35, Pages 1261-1286, Underground Globalization: Mapping the Space of Flows of the Internet Adult Industry (Zook Depo Exh. 2)
D 390	Google Directory (Zook Depo Exh. 3)
D 391	Zook1_Get_Google_Member_ List (Zook Depo Exh. 4)
D 392	The Internet, Old Hierarchies or New Networks of Centrality (Zook Depo Exh. 5)
D 393	Domains Without Whois Information (Zook Depo Exh. 6)
D 394	Domains With Whois Location Data (Zook Depo Exh. 7)
D 395	The Web of Production: The Economic Geography of Commercial Internet Content Production in the United States (Zook Depo Exh. 8)
D 396	Zook1_Get_Whois_List (Zook Depo Exh. 9)
D 397	The Geography of the Internet Industry by Matthew A. Zook (Zook Depo Exh. 10)
D 398	Excerpt from Website, Teenage Research Unlimited (“TRU”) About TRU (Our Work) (Mann Depo Exh. 2)
D 399	Excerpt from Website, The TRU Study (Study Methodology) (Mann Depo Exh. 3)
D 400	Excerpt from Website, The TRU Study (Subscription Snapshot) (Mann Depo Exh. 4)
D 401	Excerpt from Website, TRU (Client List) (Mann Depo Exh. 5)
D 402	Report - Personal Finance 2006, Executive Summary by JA Worldwide dated April 18, 2006 (Mann Depo Exh. 6)
D 403	Report - PEW Internet & American Life Project, Teens and Technology by Amanda Lenhart, Mary Madden, Paul Hitlin dated July 27, 2005 (Mann Depo Exh. 7)
D 404	Excerpt from Website, Internet Retailer, News Story from Friday, May 12, 2006 (Mann Depo Exh. 7A)
D 405	Questionnaire Form (Mann Depo Exh. 9)
D 406	The TRU Study, Online Purchases (Mann Depo Exh. 10)
D 407	All Access, Visa Debit Card (Mann Depo Exh. 10A)
D 408	Excerpt from Website, All Access, Frequently Asked Questions (Mann Depo Exh. 11)

D 409	Excerpt from Book, Credit Cards on Campus, The Social Consequences of Student Credit Dependency (Mann Depo Exh. 12)
D 410	Excerpt from Website, All Access, Terms and Conditions, Cardholder Agreement (Mann Depo Exh. 13)
D 411	Report - Over the Brink: Credit Card Debt and Bankruptcy dated June 28, 2006 (Mann Depo Exh. 14)
D 412	Report - Regulating Information dated June 13, 2006 (Mann Depo Exh. 15)
D 413	Story - Look Who's Whipping Out The Card: High Schoolers Full Story by Joylayne Houtz (Mann Depo Exh. 16)
D 414	News Article - FIRM Card Puts Emphasis on Teenage Money Management Skills by Cards International dated August 9, 2005 (Mann Depo Exh. 17)
D 415	Article - Debit Card Report, A New Life for Teen Cards by David Gosnell dated August 2005 (Mann Depo Exh. 18)
D 416	Story - NetSpending, Prepaid Card Combines Online Services, Ease of Debit for Bank-wary Consumers by Lori Hawkins dated June 19, 2006 (Mann Depo Exh. 19)
D 417	Story - Babies Receiving Credit Card Applications by TheDenverChannel.com dated June 2, 2006 (Mann Depo Exh. 20)
D 418	Story - Who Killed Richard Cullen? by Ron Ronson dated July 16, 2005 (Mann Depo Exh. 21)
D 419	COPA, Report to Congress dated October 20, 2000 (Mann Depo Exh. 22)
D 420	Article - William and Mary Law Review, The Promise of Internet Intermediary Liability by Ronald J. Mann, Seth R. Belzley dated October 2005 (Mann Depo Exh. 23)
D 421	The University of Texas School of Law, Law and Economics Working Paper No. 045, The Promise of Internet Intermediary Liability by Ronald J. Mann, Seth R. Belzley dated April 2005 (Mann Depo Exh. 24)
D 422	Excerpt from Website, AtariBoy Bypassing School Filter and Blocks dated January 1, 2006 (Felten Depo Exh. 3)
D 423	Curriculum Vitae of Andrew Gelman, Ph.D. (Gelman Depo Exh. 3)
D 424	The Polls-A Review, Preelection Survey Methodology: Details From Eight Polling Organizations, 1988 and 1992 by D. Stephen Voss, Andrew Gelman, Gary King (Gelman Depo Exh. 5)
D 425	MSN 2004 Microsoft Internet Child Safety Research by ISG (Gelman Depo Exh. 6)
D 426	Reference Guide on Survey Research by Shari Seidman Diamond (Eisenach Depo Exh. 3)

D 427	Excerpt from Security/Parental Controls Omnibus - July 2003 (Eisenach Depo Exh. 4)
D 428	Excerpt from AOL Parental Control by Benenson Strategy Group dated August 21, 2002 (Eisenach Depo Exh. 5)
D 429	Excerpt from MSN Safety & Security Comprehensive Qualitative Findings by Ben Werzinger (Eisenach Depo Exh. 6)
D 430	MSN 2004 Microsoft Internet Child Safety Research by ISC (Eisenach Depo Exh. 7)
D 431	Kids Outsmart Web Filters by Stefanie Olsen dated April 19 2006 (Eisenach Depo Exh. 8)
D 432	USA Today - Cellphone Technology Rings in Pornography in USA (Eisenach Depo Exh. 9)
D 433	The Progress Freedom Foundation, Progress on Point, Parents Have Many Tools to Combat Objectionable Media Content by Adam Thierer dated April 2006 (Eisenach Depo Exh. 10)
D 434	COPA Implementation MasterCard Discussion Guide dated January 23, 2006 (redacted) (Clark Depo Exh. 4)
D 435	E-mail from Heidi Davidson to art.clark@busdyn.com (re: Prepaid/Credit Card Stats) dated February 2, 2006 (redacted) (Clark Depo Exh. 5)
D 436	Article from The Wall Street Journal, Preparing for Plastic dated January 16, 2006 (Clark Depo Exh. 7)
D 437	Report - PEW Internet & American Life Project, Youth Are Leading The Transition to a Fully Wired and Mobile Nation by Amanda Lenhart, Mary Madden, Paul Hitlin dated July 27, 2005 (Clark Depo Exh. 8)
D 438	Figures from The TRU Study, Wave 47, Spring 2006 (Clark Depo Exh. 9)
D 439	In re Visa Check/Mastermoney, No. CV-96-5238, Settlement Agreement (Clark Depo Exh. 11)
D 440	Conference - Underbanked Financial Services Forum dated June 7-9, 2006 (Clark Depo Exh. 12)
D 441	Article - Visa Building Reloadable Product Network by Daniel Wolfe dated March 20, 2006 (Clark Depo Exh. 13)
D 442	Article - eMarketer, Online Privacy and Security: The Fear Factor dated April 2006 (Clark Depo Exh. 14)

VII. Legal Issues and Pleadings

Pursuant to Pretrial Order No. 27, a separate list of objections to trial exhibits and witnesses will be filed on October 9, 2006. The Court also has advised the parties that counter designations are due, as a supplement to the pretrial order, by October 9, 2006.

Defendant's Motion to Dismiss and, in the Alternative, for Partial Judgment on the Pleadings is pending before the Court.

There are no other special legal issues or amendments to the pleadings not otherwise set forth.

VIII. Trial Time

In the event that the Court permits the use of the deposition designations listed in Section IX below, Plaintiffs estimate that their case-in-chief will take eight to ten trial days and that their rebuttal case will take one to two days. In the event that the Court does not permit the deposition designations, Plaintiffs' case-in-chief will take an estimated additional three trial days. Defendant estimates that he will require twelve trial days to present his case-in-chief. Defendant reserves the right to present any necessary rebuttal or sur-rebuttal testimony.

IX. Discovery Evidence and Trial Depositions

A. Proffered by Both Parties: Discovery Evidence

1. Plaintiffs' Contention Interrogatories and attachments thereto.

2. All of plaintiffs' responses to defendant's interrogatories.

3. Defendant's Second Supplemental Response to Plaintiffs' First Set of Contention Interrogatories dated September 27, 2006.

4. Defendant's Supplemental Response to Plaintiffs' First Set of Contention Interrogatories dated August 14, 2006, including exhibits to Contention Interrogatories 4 and 5.

5. Defendant's Supplemental Response to Plaintiffs' Initial Interrogatories dated March 16, 2006

6. Defendant's Supplemental Response to Plaintiffs' Initial Interrogatories dated March 13, 2006.

7. Defendant's Responses and Objections to Plaintiffs' Requests to Admit, February 24, 2006, Responses 1-8, 14-21, 22-24.

8. Defendant's Supplemental Responses to Plaintiffs' Initial Interrogatories dated January 27, 2006.

B. Discovery Evidence and Trial Depositions Proffered by Plaintiffs

Plaintiffs propose excerpts from ten discovery depositions. A list of those depositions and a summary of the testimony is attached to Plaintiffs' Memorandum of Law in Support of Motion to Designate Deposition Testimony Pursuant to Federal Rule of Civil Procedure 32, also being filed today. The list is contained in the Motion rather than in the Pretrial Order because it contains material designated confidential by third parties. Thus both the Motion and the attachment are being filed under seal.

Respectfully submitted,

_____ /s/_____

Christopher A. Hansen
Aden Fine
Benjamin Wizner
Catherine Crump
American Civil Liberties Union
125 Broad Street – 18th floor
New York, NY 10004

(212) 549-2693

_____/s/_____
Christopher Harris
Seth Friedman
Katharine Marshall
Jeroen van Kwawegen
Latham & Watkins LLP
885 Third Avenue
New York, NY 10022
(212) 906.1800

For Plaintiffs

_____/s/_____
Theodore C. Hirt
Raphael O. Gomez
Eric J. Beane
Isaac Campbell
Joel McElvain
Kenneth Sealls
James D. Todd, Jr.
Tamara Ulrich
United States Department of Justice
Civil Division, Room 6144
20 Massachusetts Ave. NW
Washington D.C. 20530

For Defendant

CERTIFICATE OF SERVICE

I hereby certify that on October 3, 2006, I electronically filed the foregoing documents with the Clerk of the Court using the ECF system, which will send notification of such filing to Raphael O. Gomez, Department of Justice.

____/s/_____
Jeroen van Kwawegen
Latham and Watkins
885 Third Avenue
New York, NY 10022

Counsel for Plaintiffs